Cyber Compendium

Rob Hulsebos

PHOENIX CONTACT
INSPIRING INNOVATIONS

INTRODUCTIE

Dat er virussen bestaan, weet elke PC-gebruiker tegenwoordig wel. Dat een beveiliging noodzakelijk is om te voorkomen dat de bankrekening geplunderd wordt, is ook eigenlijk wel bekend. Soms zien we op TV weer een reportage over een nieuwe “hack” en het lijkt allemaal wel mee te vallen want verder horen we er meestal weinig meer over. Maar de consequenties van sommige “hacks” zijn vérreikend; bijvoorbeeld het opruimen van de schade van de “DigiNotar” inbraak kostte de Nederlandse overheid meer dan een jaar. De toenemende afhankelijkheid van IT-systemen maakt de maatschappij steeds kwetsbaarder voor cybersecurityproblemen. En sinds “Stuxnet”, het eerste industriële virus, richt de aandacht van hackers zich meer-en-meer op de industrie.

Cybersecurity is eigenlijk niets meer dan een extra stap bij de gewone beveiligingsmaatregelen in een bedrijf: hek, portier, receptie, bewaking, detectoren, speciaal glas, etc. Vanzelfsprekend toch? Waarom dan geen drempels opwerpen voor hackers en cybercriminelen? “Hollywood” doet het voorkomen alsof hackers, allemaal superintelligent, met een paar toetsaanslagen kunnen inbreken. Onzin! De meeste hackers maken slechts gebruik van de onwetendheid en onkunde van de gemiddelde gebruiker. Hackers zijn niet slim; wij zijn wel vaak digitaal dom.

Uiteraard is het in kort bestek niet mogelijk om de sterktes en zwaktes van alle dagelijks gebruikte technologieën op te sommen en een hierop afgestemd compleet beveiligingsplan te schrijven. Dat is ook niet het doel van dit werk. De eerste helft van dit boekje is daarom bedoeld om in gewoon Nederlands een inleiding te geven in de veelomvattende wereld van de industriële cybersecurity en “hacken”, waarom dit kan, wat er allemaal mogelijk is, voor welke uitdagingen de industrie staat, gevolgd door wat tips om er iets aan te doen.

Het tweede deel van het boekje houdt zich alleen maar bezig met het jargon uit de cybersecuritywereld: “Trojan”, “Ping of death”, “Worm”, “Forever Day” enzovoorts. Deze worden hier kort en krachtig uitgelegd omdat vaak in de verste verte niet te raden is wat het ook maar zou kunnen zijn.

Hopelijk geeft dit werk een bruikbare introductie op de dynamische wereld van de cybersecurity. Deze eerste versie is ongetwijfeld niet compleet. Suggesties, verbeteringen en voorstellen voor uitbreidingen zijn uiteraard zeer welkom bij de auteur (op onderstaand adres) of Phoenix Contact B.V.

E-mail: r.hulsebos (at) onsnet.nu

Compendium

het compendium zelfst.naamw.
Uitspraak: [kɔm'pɛndijʏm]
Verbuigingen: compendium|s, compendi|a (meerv.)

1. *Handboek met een samenvatting van de kennis op een bepaald terrein*
2. *Handboek of overzicht dat de hoofdzaken en begrippen van een wetenschap, vakgebied of onderwerp beknopt maar veelomvattend weergeeft.*

Over de auteur

Rob Hulsebos (1961) studeerde HTS Informatica met een specialisatie in datacommunicatie. Sinds 1984 is hij werkzaam (geweest) bij de R&D afdelingen van diverse bedrijven om producten voor industriële netwerken te ontwikkelen en toe te passen in machines. De hiermee opgedane praktijkervaring heeft geleid tot de publicatie van meer dan 250 artikelen in de vakpers en drie boeken over dit onderwerp. Tevens geeft hij cursussen op zijn vakgebied en is regelmatig gastspreker op seminars, congressen en bij bedrijven. In 2010 hielp hij mee bij de ontcijfering van het Stuxnet virus en publiceert sindsdien over actuele ontwikkelingen rondom industriële cybersecurity in het vakblad “Automatie”.

Over Phoenix Contact

De wereld van Phoenix Contact is de wereld van de aansluittechniek tussen aders en printplaten, de wereld van de automatiseringstechniek, de elektrische interfacetechniek en de wereld van de overspanningsbeveiliging. Wereldwijd geven in totaal 13.000 medewerkers deze wereld samen met klanten en bedrijfspartners vorm.

In de wereld van morgen zijn productie systemen communicatief, intelligent, zelfstandig en digitaal transparant. Dat betekent dat er dan geen centrale besturing meer is, maar een intelligent samenwerken waardoor het systeem onmiddellijk reageert met een adequate aanpassing van het productieproces. Om dit te kunnen bewerkstelligen is een veilige industriële communicatietechniek van essentieel belang. Ethernet en internet vormen een goede basis daarvoor, mits goed beveiligd!

Phoenix Contact biedt u hiervoor een breed programma Industrial Ethernet-producten aan, waarmee u alle mogelijkheden die Ethernet-netwerken te bieden hebben kunt benutten. Industrial Ethernet van Phoenix Contact kunt u gemakkelijk in uw automatiseringsinfrastructuur integreren, want wij maken Ethernet eenvoudig.

INHOUD

HOOFDSTUK I

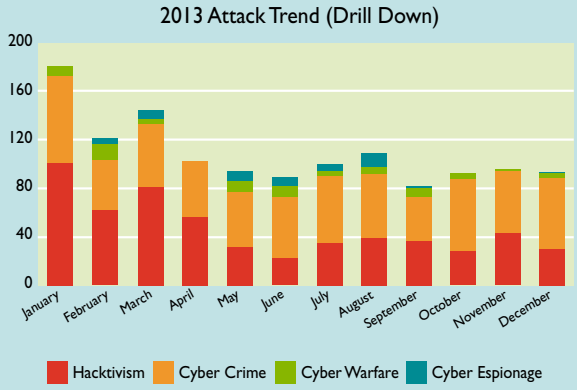
CYBERSECURITY

1. CYBERSECURITY

Technologie kan ons dagelijks leven vereenvoudigen, maar het ligt ook in de menselijke aard om elke bestaande technologie voor het verkeerde doel in te zetten. De IT is daarin bepaald geen uitzondering gebleken. De alomvattende aanwezigheid van IT-systemen in alle aspecten van de huidige maatschappij maakt dat hier ook misbruik van gemaakt wordt. Hier wordt vaak het woord "hacken" voor gebruikt, wat in de oorspronkelijke betekenis niet meer inhoudt dan: iets doen met een apparaat waarvoor het oorspronkelijk niet bedoeld was.

Inmiddels hangt er wel een negatieve associatie rondom de activiteit (hacken) en degenen die het doen (hackers). Maar niet elke hacker is persé op andermans geld uit; sommigen doen het vanwege de technische uitdaging, anderen vanuit maatschappelijke betrokkenheid met een bepaald thema ("hacktivisme"), weer anderen willen de slechte beveiliging van IT-systemen aan de orde stellen en sommigen willen gewoon extra mogelijkheden aanspreken in apparatuur die ze gekocht hebben. Maar er zijn er ook die wel op geld, bezittingen of informatie uit zijn of bepaalde (machts)politieke doelen nastreven.

Hacktivisme



PRAKTIJKVOORBEELD

◀ Soorten cyberaanvallen in 2013, geclassificeerd naar type *(bron: www.hackmageddon.com)*

Om duidelijk te maken dat niet elke hacker een (cyber)crimineel is worden hier kreten als “white hat hacker”, “responsible hacker”, “ethical hacker” etc. gebruikt, dit als onderscheid van de “black hat hackers” die wel met de meer duistere zaken bezig zijn. Dan hebben we het over “cybercrime”.

Volgens beveiligingsbedrijf Kaspersky waren in 2013 cyberdreigingen de tweede grootste risicofactor voor bedrijven, direct volgend op de economische onzekerheden. Maar meer dan 40% van de ondernemingen had in 2013 nog geen enkele maatregel genomen op dit gebied. Maatregelen zijn zeker nodig, aangezien bedrijven steeds meer afhankelijk zijn van een goed functionerend IT, zowel ‘op kantoor’ als ‘op de fabrieksvloer’.

1.1 WAT IS CYBERSECURITY

Als consument komen we met sommige van de hierboven genoemde zaken in aanraking, als bedrijf weer met andere. Uiteraard is het verstandig om zich hiertegen te beschermen; net zoals een slot op de voordeur, een alarmsysteem, een bewakingsdienst, etc. kunnen ook IT-systemen beveiligd worden tegen hackers. Een absolute 100% beveiliging is niet haalbaar; net zoals met de gewone criminaliteit is er een haasje-over tussen beveiligingstechnieken en criminelen. Een nieuwe beveiligingsmethode helpt even, totdat ook hier de zwakke plekken weer in ontdekt zijn.
Onder cybersecurity verstaan we het collectief van maatregelen om een IT-infrastructuur te beveiligen tegen de hierboven genoemde vormen van misbruik. Cybersecurity maatregelen kunnen bestaan uit:

Firewall

- Technische maatregelen: virusscanners, firewalls, monitoring, ...
- Procedurele maatregelen: standaarden, audits, backup procedures, ...
- Personele maatregelen: opleidingen, bewustwording, ...

Wat voor een bepaald systeem de beste oplossing is, is niet van te voren te bepalen. Meestal wordt direct gedacht aan

het technische aspect, maar dat is maar een (klein) deel van het geheel. Procedurele en personele maatregelen zijn vaak veel belangrijker, maar kosten meer moeite en zijn minder 'sexy' dan de allernieuwste beveiligingshardware en -software. In een technische omgeving, zoals de industriële IT is, zijn de procedurele en personele aspecten van cybersecurity vaak onderbelicht. Hackers maken daarom ook graag gebruik van "social engineering", waarbij persoonlijk contact gezocht wordt met het (aanstaande) slachtoffer en via gesprekstechnieken informatie wordt ontfutseld, of overgehaald wordt bepaalde handelingen uit te voeren om zodoende op zijn/haar systeem in te kunnen breken.

PRAKTIJKVOORBEELD

De hacker belt een willekeurig telefoonnummer en doet zich voor als "een medewerker van Microsoft", die zogenaamd heeft geconstateerd dat er een virus op uw PC staat. Het is dan de bedoeling dat u naar een bepaalde website gaat "om de PC te ontsmetten". Wat er feitelijk gebeurt is dat met uw bereidwillige hulp malware op de PC geladen gaat worden. Daarna kan de hacker de PC op afstand overnemen voor andere doeleinden.

Technische maatregelen en apparatuur helpen niet tegen dit soort aanvallen. Dat bewustwording bij gebruikers nodig is, bewijst een onderzoek van het Idaho National Laboratory (VS):

- 20% van de medewerkers stopt een op straat gevonden USB-stick zó in zijn PC.
- 22% klikt op elke 'leuke' link in een e-mail.
- 40% geeft over de telefoon zijn wachtwoord.

WEBSITE

De website www.socialengineering.nl geeft meer uitleg over de vormen van social engineering en hoe men zich hiertegen verdedigen kan.

Het is niet voor niets dat hackers deze drie methodes graag gebruiken om een cyberaanval te beginnen. Maar het kan ook nog anders: geautomatiseerd. Met speciale softwaregereedschappen (tools) is het mogelijk om geheel automatisch systemen te laten controleren op alle bekende beveiligingslekken en indien er een gevonden wordt is deze direct te misbruiken. Deze tools bestaan uiteraard voor Windows, Linux, MacOS, etc. maar óók voor industriële besturingen. Het vereiste kennisniveau om in een systeem binnen te komen is vrij laag, zeker als zo'n systeem niet de laatste softwareversie en de juiste configuratie heeft.

Enkele voorbeelden van zulke tools zijn:

- Kali Linux (www.kali.org)
- Agora SCADA+ (www.gleg.net/agora_scada.shtml)

MetaSploit

- MetaSploit (www.metasploit.com)
- Nessus (www.tenable.com/products/nessus)

Alle genoemde tools zijn overigens bedoeld voor beveiligingsonderzoekers, niet voor hackers.

TIP

Het is zeer leerzaam om met deze tools te werken; van Kali, MetaSploit en Nessus zijn vereenvoudigde versies gratis op te halen op de genoemde websites.

Behalve tools heeft een hacker ook nog een besturing nodig om op in te breken. De zoekmachines Google en Shodan maken het eenvoudig om automatisch bepaalde soorten apparaten die op het internet zijn aangesloten, te vinden *(zie ook "incident 5" in hoofdstuk 4)*.

1.2 VORMEN VAN HACKEN

Uiteraard hebben de maatschappij, bedrijven en personen geen last van de white/responsible/ethical hackers. De andere categorieën hackers zijn ons wel tot last, op een veelvoud

van manieren. De software die zij hiervoor gebruiken wordt met de verzamelnaam “malware” aangeduid: een samenvoeging van de woorden “malicious” en “software”, software met een kwaadaardig karakter dus. In het dagelijkse taalgebruik wordt vaak van “computervirussen” (of gewoon: “virussen”) gesproken.

Malware

In het vakgebied cybersecurity wordt nog een gedetailleerder onderscheid gemaakt, naar de manier waarop besmetting plaatsvindt en de verdere verspreiding geregeld wordt:

Trojan	Software die nuttig lijkt voor een bepaalde taak, maar daarnaast ook nog malware bevat. Besmetting vindt plaats door e-mails met bijlagen, of door het bezoeken van besmette websites. Een trojan verspreidt zich verder niet.
Virus	Malware die zichzelf kan verspreiden met hulp van de gebruiker, bijvoorbeeld via een besmette USB-stick die in een ander systeem gestoken wordt.
Worm	Malware die zichzelf zelfstandig verder kan verspreiden, bijvoorbeeld via internet of een LAN. Verspreiding kan dan ook zéér snel gaan.

Trojan
Virus
Worm

Voor de gemiddelde gebruiker is het onderscheid vaag en worden alle vormen van malware aangeduid als “virus”. Een virusscanner zal wel alle genoemde soorten malware detecteren. Wat een trojan / virus / worm verder doet, staat los van de methode van besmetting en verspreiding en wordt verder bepaald door de programmeur ervan. Enkele voorbeelden van wat malware kan doen:

Virusscanner

Adware
Malware die (veelal op ongewenste) momenten advertenties in een browser laat zien, ook al heeft de gebruiker dit in de browser uitgezet.

Diefstal (meestal van geld)

Politievirus

Malware die tijdens het internetbankieren probeert mee te liften op een transactie om een extra geldbedrag over te maken. Gijzel- of politievirussen melden dat u met iets illegaals bezig bent en blokkeren de PC tot een bepaald geldbedrag (naar het buitenland) is overgemaakt.

Fraude

Malware die persoonlijke informatie (rekeningnummers, wachtwoorden, pincodes, creditcardgegevens, etc.) verzamelt, waarna op rekening van het slachtoffer aankopen worden gedaan, geld wordt opgenomen, etc. Ook kan de beveiliging van debetkaarten worden omzeild zodat er geld op gezet kan worden om daar weer aankopen mee te doen.

Kopiëren van vertrouwelijke gegevens

Malware die op zoek gaat naar interessante informatie (financiële gegevens, broncodes, documenten, intellectueel eigendom, etc.), om deze dan door te sturen naar een externe server. Ook kunnen toetsaanslagen worden opgeslagen of screendumps worden gemaakt. Dit kan een vorm van bedrijfsspionage zijn.

Zulke malware is vaak erg ‘stil’; er wordt weinig netwerkverkeer gegenereerd en er ontstaat geen extra CPU belasting. Daarom kan zulke malware jarenlang onopgemerkt in een bedrijf actief zijn, om zodoende honderden gigabytes aan data te kunnen wegsturen.

Wissen van gegevens / harde schijven

In de 90’er jaren was het wissen van de harde schijf een populaire actie van virussen. Ook kunnen bestanden ‘gegijzeld’ worden door de inhoud te coderen; het slachtoffer kan alleen na betaling van een bedrag de decodeersleutel krijgen.

In 2012 was oliemaatschappij Saudi Aramco getroffen door een virus dat uiteindelijk al op 30000 PC's bleek te staan en op het punt stond van elke PC de harde schijf te wissen.

BUG

Aanpassen van gegevens / programmatuur, saldi, (batch)recepten, etc.
Deze vorm van hacken wordt vaak vereenvoudigd doordat bedrijven gebruikersaccounts niet verwijderen en/of wachtwoorden niet veranderen nadat personeel ontslagen is. Uit rancune worden dan soms bestanden gewist, instellingen gewijzigd of op afstand de besturing overgenomen.

Twee personeelsleden van de gemeente Los Angeles herprogrammeren de centrale besturing voor de stoplichten in het centrum, vanwege onvrede over de CAO-onderhandelingen. Het leidt tot een complete verkeerschaos in de stad omdat veel stoplichten nog maar zelden 'groen' geven.

PRAKTIJKVOORBEELD

Hacktivisme
Het uitvoeren van een hack op de infrastructuur van een bedrijf of instelling, vanwege een zakelijk of politiek meningsverschil met dat bedrijf of het land waar het in gevestigd is. Veelal gaat het om het aanpassen van een website zodat de normale webpagina's vervangen worden door een boodschap van de hacker (een soort digitale graffiti eigenlijk). Omdat veel websites slecht beveiligd zijn, is dit relatief eenvoudig te doen.

Hacktivisme

Denial of Service
Het functioneel blokkeren van een systeem door een overbelasting (van netwerkverkeer, van webservers, e-mail servers etc.). Na afloop van de DoS-aanval is het systeem gewoon weer beschikbaar.

Denial of Service

DoS

Fysieke beschadiging van apparatuur

Het door overbelasting of oververhitting beschadigen van apparatuur zodat deze defect raakt. Meestal is dit vrij moeilijk op een PC, tablet of mobiele telefoon. Maar in industriële toepassingen is er veel meer mogelijk; het bekendste voorbeeld hiervan is het Stuxnet virus, dat speciaal gemaakt is om een uraniumverrijkingsfabriek te saboteren *(zie ook hoofdstuk 5)*.

Stuxnet
Virus

Transmissie van malware of spam

Het gebruik maken van een systeem van iemand anders om malware of spam te versturen naar anderen, zodat de hacker dit niet van achter zijn eigen systeem hoeft te doen en dus ook niet te vinden is. Het spoor loopt dan dood op het systeem van het (veelal onwetende) slachtoffer.

Malware

Als veel systemen voor dit werk nodig zijn, wordt door de hacker een "botnet" opgezet, die op afstand te besturen zijn. Botnets kunnen uit wel honderdduizenden systemen bestaan, waarmee massieve hoeveelheden data verstuurd kunnen worden. Ook kunnen websites aangevallen worden die dan overbelast raken door de gelijktijdige bezoekers. Botnets kunnen, voor een luttel bedrag, online gehuurd worden van hierin gespecialiseerde cybercriminelen.

Botnet

Identiteitsdiefstal

Het zich voordoen als iemand anders. Op internet speelt het elektronisch correct kunnen vaststellen van de identiteit van iemand "aan de andere kant" een belangrijke rol, omdat er geen zichtcontact is. Daarom wordt met digitale certificaten gewerkt, waarmee iemand zijn identiteit kan aantonen.

Het bedrijf dat deze certificaten in Nederland leverde, Diginotar, was door een Iraanse hacker aangevallen en als gevolg hiervan kon geen enkel digitaal certificaat meer worden vertrouwd. De omwisseling van alle Diginotarcertificaten door nieuwe certificaten heeft een jaar geduurd.

Cyberwar

Cyberoorlogsvoering

Het aanvallen van IT-systemen van de tegenstander, met

als doel deze op afstand onschadelijk te maken (vliegtuigen, schepen, communicatienetwerken, drones, radars, etc).

In 2012 ontstaat ophef in de VS als blijkt dat wereldwijd verkochte GSM-communicatieapparatuur van sommige Chinese firma's mogelijk op afstand afgeluisterd of uitgeschakeld zou kunnen worden. Ook bepaalde merken PC's raken verdacht.

PRAKTIJKVOORBEELD

Cyberoorlogsvoering staat sterk in de belangstelling sinds Stuxnet, omdat hiermee goedkoop en snel politieke doelen kunnen worden bereikt zonder dat voor het slachtoffer duidelijk is wie er achter zit.

Stuxnet

Is alle malware slecht?

Het lijkt een retorische vraag, maar het antwoord is niet altijd vanzelfsprekend "ja". Veel malware is (nog steeds) gericht op particulieren en/of bedrijven, maar niet specifiek gemaakt om een industriële omgeving aan te vallen. Uiteraard is het vervelend als een PC malware bevat die een extra bedrag afboekt tijdens internetbankieren, maar wie zijn industriële PC niet gebruikt voor privézaken heeft er verder geen last van.

Malware

Desalniettemin is het toch ongewenst om malware op een industriële installatie te hebben, want wat vandaag niet schadelijk is, kan het morgen wel zijn. Preventie en bestrijding ervan blijft nodig. Omdat in de industrie veel van dezelfde technologie gebruikt wordt als in de zakelijke / consumenten IT, is het noodzakelijk te volgen wat hier allemaal aan malware ontdekt wordt.

HOOFDSTUK 2

SOFTWARE MISBRUIKEN

2. SOFTWARE MISBRUIKEN

2.1 KRAKEN VAN BRANDKASTEN EN SOFTWARE

Wanneer een inbreker een brandkast wil kraken moet hij eerst een manier vinden om ongezien voorbij de portier te komen waarna hij op verschillende manieren door de beveiliging van een brandkast heen kan breken: a) de “brute force” methode met een thermische lans of met dynamiet; b) misbruik maken van een ontwerpfout om het slot open te krijgen; of c) de code weten te vinden, dan wel d) iemand verleiden / bedreigen om de code te geven.

Brute force

Bij een hacker gaat het eigenlijk niet anders. Een hacker die misbruik wil maken van, of in wil breken op een systeem gebruikt dezelfde technieken. Om door de beveiliging heen te breken, kan gebruik gemaakt worden van: a) zwaktes in de software, bijvoorbeeld met een ‘brute force” aanval wachtwoorden raden, of b) gebruik maken van een ontwerpfout

of codeerfout in de software, of c) kijken of er een briefje onder het toetsenbord zit, of d) een gebruiker overhalen om zijn wachtwoord opnieuw in te geven “ter verificatie”.

De consequentie in beide voorbeelden is dat door de beveiliging heen gebroken wordt. Om te weten hoe zulke aanvallen weerstaan kunnen worden, is inzicht nodig in hoe een hacker misbruik kan maken van lekken in software, of fouten in het gebruik ervan. Hoe precies een beveiliging gebroken wordt, hangt af van de gebruikte software: netwerkprotocollen vereisen een andere aanpak dan websites, databases, embedded systemen, etc. Denk hierbij onder andere aan:

- Programmeerfouten;
- Ontwerpfouten;
- Architectuurfouten.

Deze fouten worden gemaakt door de programmeurs en/of ontwerpers tijdens het maken van de software. Eenmaal in gebruik, kan zelfs kwalitatief goede software nog zwaktes vertonen, bijvoorbeeld vanwege:

- Configuratiefouten;
- Gebruiksfouten;
- Overbelasting.

Voor hackers is de eerste categorie fouten het meest interessant; immers, is er eenmaal een systeem gevonden met zo’n fout, dan is direct bekend dat alle systemen met diezelfde software kwetsbaar zijn. Maar ook de fouten uit de tweede categorie worden graag door hackers gebruikt - als een bedrijf cyberveilige software oplevert, dan kunnen duizenden klanten allemaal die ene beginnersfout maken waardoor een systeem toch kwetsbaar wordt.
Verder staat de stand van de technologie natuurlijk niet stil (bijvoorbeeld: snellere processoren, nieuwe wiskundige algoritmes) en het kan dus voorkomen dat een systeem dat vroeger goed beschermd was, dat op een bepaald moment niet meer is (eigenlijk een soort “veroudering” van software dus).

WiFi (draadloos Ethernet) werkte vroeger met het "WEP" encryptiealgoritme. Dankzij "brute force" rekenwerk op steeds snellere processoren en met wiskundige optimalisaties kan een WEP wachtwoord tegenwoordig binnen een seconde worden ontsleuteld. WEP beveiliging op draadloze netwerken is daarom compleet ontoelaatbaar geworden.

ALARM

Tenslotte kunnen bepaalde snufjes in software, die ooit bedacht waren vanwege het nut voor de (eind)gebruiker, vanaf een bepaald tijdstip zodanig door hackers misbruikt gaan worden dat deze functionaliteit voortaan maar beter uitgeschakeld kan worden.

"Autorun" is een functie van Windows waarbij deze scant wat er op een USB-stick, DVD of CD-ROM staat en dan de bijbehorende programmatuur uitvoert. Bijvoorbeeld, een film kan automatisch afgespeeld worden, software automatisch geïnstalleerd, etc. Hackers gebruiken "autorun" dus graag voor installatie van malware. Daarom heeft Microsoft de functie nu standaard uitgezet (gebruikers kunnen dit nog wel wijzigen).

PRAKTIJKVOORBEELD

2.2 PROGRAMMEERFOUTEN

Programmeerfouten in software zijn een van de meest voorkomende oorzaken van beveiligingslekken in software. Het gaat hierbij niet om een functionele fout (bijvoorbeeld, in schrikkeljaren februari ook maar 28 dagen geven), die zijn op zich vervelend of lastig maar niet de oorzaak van een beveiligingslek. De fouten waar we wel last van hebben zijn op zich vaak erg onschuldig, tijdens normaal gebruik van de software heeft niemand er last van; de software doet verder ook gewoon wat ze moet doen. Maar een hacker kan de software op een andere manier gebruiken, data aanleveren, functies uitvoeren etc. op een manier die de oorspronkelijke programmeur niet heeft voorzien en ook niet detecteert.

Het Amerikaanse MITRE (Massachusetts Institute of Technology Research & Engineering) houdt een website hierover bij met de "Top 25 van 's werelds meest gevaarlijke softwarefouten". Op nr. 1 en op nr. 2 staan twee fouten gerelateerd aan het programmeren van webservers. Op nr. 3 staat de meest gevaarlijke fout voor industriële software: de "buffer overflow".

2.2.1 DE BUFFER OVERFLOW

Een buffer overflow ontstaat als een programma te weinig geheugenruimte reserveert voor de opslag van data die het aangeleverd krijgt (bijvoorbeeld via een netwerk, of invoer via een toetsenbord, etc.).

PRAKTIJKVOORBEELD

Stel een programmeur moet in staat zijn een 4 cijferige pincode in te lezen voor controle. Hij reserveert voor de opslag hiervan dan 4 bytes (karakters) in het geheugen, dat zou genoeg moeten zijn. Maar wat gebeurt er nu als diegene achter het toetsenbord na 4 cijfers gewoon doorgaat met typen? Als het programma hierop niet controleert, worden alle extra cijfers ook in het geheugen opgeslagen. Maar omdat er maar voor 4 karakters bufferruimte was, gaan de extra karakters andere data overschrijven. Hierdoor neemt het programma misschien later verkeerde beslissingen, of stopt het.

De ervaring leert dat veel programmeurs niet goed omgaan met controles op invoer van data; ook buffer overflows ontstaan erg eenvoudig. Zelfs voor ervaren programmeurs is het nog eenvoudig om zulke fouten te maken. Een belangrijke reden hiervoor is dat bepaalde programmeertalen die voor industriële toepassingen en embedded software veel gebruikt worden, zoals C en C++, de programmeur in het geheel niet assisteren op dit gebied.

De buffer overflow is maar één van de vele soorten fouten die een programmeur kan maken; een ander die veel gemaakt wordt is geen controle op invoer (geen invoervalidatie). Denk hierbij o.a. aan geldige data, productiehoeveelheden, geen negatieve waardes mogelijk op bepaalde invoer, etc. Een ingewerkte operator zal zulke fouten misschien niet maken, zodat het gebrek aan invoervalidatie niet opvalt. Maar hackers maken graag gebruik van deze omissies.

Geen of gebrekkige invoervalidatie is ook een belangrijke bron van beveiligingsproblemen in de software van netwerkprotocollen. Deze dienen elk netwerkbericht te controleren op geldige inhoud in *alle* velden.

PRAKTIJKVOORBEELD

Een eenvoudig voorbeeld van een falende invoervalidatie is op de lengte van een netwerkbericht. Zo was ooit Windows NT eenvoudig te crashen door het een "ping of death" te sturen, namelijk een netwerkbericht dat veel langer was dan verwacht.

```
>ping -l 65000 192.168.1.1

Pinging 192.160.1.1 with 65000 bytes of data:
Reply from 192.168.1.1: bytes=65000 time=18ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=18ms TTL=64
Reply from 192.168.1.1: bytes=65000 time=18ms TTL=64
Reply from 192.160.1.1: bytes=65000 time=10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli seconds:
    Minimum = 18ms, Maximum = 18ms, Average = 18ms
```

Dit stuurt netwerkberichten met een lengte van 65000 bytes naar een opgegeven doelwit (192.68.1.1). Nu crasht Windows er echter niet meer op.

2.2.2 EERST WEL VEILIG, NU NIET MEER

Het vervelende aan software is dat niet gegarandeerd is dat een bepaalde functie die eerst wel goed werkte, in de komende versie van die software nog steeds goed functioneert. Door het installeren van een nieuwe versie van een softwarepakket kan de veiligheid dus juist in sterkte dalen. Het hierna getoonde voorbeeld van PHP is een goed voorbeeld van hoe het fout kan gaan: een nieuwe release lost een

aantal beveiligingslekken op, maar introduceert tegelijkertijd een nieuw, zeer ernstig lek. De gebruiker zit dan in een spagaat: zowel de huidige als de nieuwe versie van de software is kwetsbaar.

PRAKTIJKVOORBEELD

PHP is een veel voor websites gebruikte programmeertaal. Toen versie 5.3.7 uitgebracht werd, moesten de ontwikkelaars het gebruik van hun eigen product ten sterkste afraden, vanwege een (nieuwe) fout in het beheer van wachtwoorden.

2.2.3 INDUSTRIEEL VOORBEELD

SCADA

De Italiaanse beveiligingsonderzoeker Luigi Auriemma gaf begin 2012 de resultaten vrij van een onderzoek naar de beveiligingslekken van een viertal SCADA-systemen. In totaal zijn 35 beveiligingslekken gevonden, waarbij per SCADA-systeem maar gedurende twee dagen gezocht is. Interessant hierbij was dat hij ook gekeken heeft naar de mogelijke oorzaak van de gevonden beveiligingslekken.

De onderstaande tabel geeft voor de 4 leveranciers A,B,C en D de oorzaak van beveiligingslekken:

Type fout	A	B	C	D
Buffer overflow	2	-	5	6
Invoervalidatie	1	11	1	-
Geheugenbeheer	-	1	-	-
Geheugencorruptie	1	-	-	-
Overig	2	1	2	1

Opvallend is dat een bepaalde programmeerfout bij het ene SCADA-systeem vaker gemaakt wordt dan bij het andere. Dit is mogelijk het gevolg van een programmeur die steeds dezelfde fout gemaakt heeft op verschillende plaatsen in de code.

De eindconclusie uit Auriemma's onderzoek is eigenlijk schokkend: dat deze vier SCADA-systemen, geschat in gebruik in ca. 1 miljoen installaties wereldwijd, door de eerste de beste onderzoeker binnen 2 dagen te kraken zijn dankzij fouten van een beginnende of onervaren programmeur. Het zegt ook iets over de methode van softwareontwikkeling bij die bedrijven. Waarschijnlijk zou Auriemma nog veel meer beveiligingslekken gevonden hebben als hij er meer tijd aan besteed zou hebben.

SCADA

2.3 ONTWERPFOUTEN

Beveiligingslekken van deze orde ontstaan dankzij een fout in het ontwerp van de software. Het is dus géén programmeerfout, maar veel fundamenteler. Dat is dus ook niet zo eenvoudig op te lossen.

De "WiFi Protected Setup" van draadloos Ethernet werkt met een 7-cijferige pincode. Dat zou dus 10 miljoen unieke pincodes moeten geven. Door een ontwerpfout blijken het er maar 11000 te zijn. Dit is zo weinig dat een hacker ze eenvoudigweg allemaal kan uitproberen. Het gebruik van WPS moet dus afgeraden worden.

PRAKTIJKVOORBEELD

2.3.1 WACHTWOORDGEBRUIK

Een eenvoudige maar desastreuze ontwerpfout is het maken van software waarvan het wachtwoord niet gewijzigd kan worden. Zodra het wachtwoord bekend wordt, hebben alle gebruikers van die software dus een serieus probleem.

BUG

De auteurs van de Stuxnet malware maakten gebruik van het bekend geworden wachtwoord van het engineering pakket en konden zo de PLC programma's in de database wijzigen.

Een ander voorbeeld van een ontwerpfout is het in leesbare tekst oversturen van wachtwoorden over een netwerk. Iedereen die meeluistert en dat netwerkbericht oppikt, is daarna dus op de hoogte van het wachtwoord.

PRAKTIJKVOORBEELD

Voorbeelden van protocollen die zo werken zijn FTP (File Transfer Protocol) en SNMP 1.0 (Simple Network Management Protocol). Alhoewel beide al 30 jaar oud zijn en de zwaktes ervan al lang bekend, worden ze nog steeds erg veel gebruikt.

MAC-adres

Een andere veelvoorkomende ontwerpfout is om beveiligingsinstellingen afhankelijk te maken van Ethernet MAC adressen in apparatuur. Een Ethernet MAC adres is het netwerkadres van het apparaat, is 48 bits groot en wereldwijd uniek (in principe). Als een apparaat met een Ethernetpoort de fabriek verlaat, heeft de leverancier het een eigen MAC-adres gegeven, waarmee het zich dus onderscheidt van alle andere apparaten van hetzelfde type. Omdat het MAC-adres uniek is, wordt het gebruikt in het algoritme om een apparaat een uniek wachtwoord te geven. Op deze manier kan elk apparaat een eigen, uniek, wachtwoord krijgen. Dit klinkt in eerste instantie precies als wat nodig is. Eenzelfde algoritme wordt wel eens gebruikt bij draadloos Ethernet, waar het wachtwoord wordt afgeleid van de netwerknaam, of het MAC-adres.

Maar als het algoritme om het wachtwoord uit te rekenen uit het MAC-adres uitlekt, kan iedereen dus het wachtwoord uitrekenen. En aangezien het MAC-adres gebruikt wordt in elk netwerkbericht dat een apparaat stuurt, is het afluisteren van één netwerkbericht dus al genoeg voor een hacker. Hetzelfde is het geval als de netwerknaam afgeleid is van het MAC-adres.

MAC-adres

Daarom wordt ook altijd het advies gegeven om een fabriekswachtwoord meteen te wijzigen na aanschaf.

TIP

Een website met een lijst van fabriekswachtwoorden is: www.cirt.net/passwords

WEBSITE

2.3.2 BACKDOORS (ACHTERDEURTJES)

Backdoor

In veel apparatuur zijn zgn. "backdoors" aangebracht door de leverancier. Hiermee kan buiten de reguliere applicatiesoftware om toegang tot de besturing gekregen worden. Dit kan om diverse redenen gedaan worden:

- Het kunnen configureren / afregelen van de apparatuur in de fabriek;
- Het configureren van de apparatuur door de klant;
- Het uitlezen van diagnostische gegevens;
- Voor uitvoeren van diagnose op afstand.

Het probleem met dit soort functionaliteit is dat ze erg nuttig is, erg krachtig is, maar ook erg gevaarlijk kan zijn indien het op de verkeerde momenten gebruikt wordt of er ongewenste commando's gegeven worden. Maar juist vanwege de krachtige mogelijkheden worden backdoors zeer gewaardeerd door software engineers, inbedrijfstellers /

afregelaars, troubleshooters, etc. In het algemeen geldt dat zij weten wat ze wel en niet moeten doen. Maar de krachtige mogelijkheden zijn voor hackers natuurlijk ook bijzonder interessant.

BUG

Een bepaald merk PLC blijkt feitelijk een Linux systeem te zijn. Via een backdoor kan iedereen beheerdersrechten krijgen. Dit biedt de mogelijkheid om alle bestanden te wijzigen, ook de PLC programma's zelf. Toegang tot alle I/O is ook mogelijk.

Backdoor

Een ander probleem met backdoors is dat ze vaak aanwezig zijn zonder dat de klant daar iets van weet. Er zullen dus ook geen beveiligingsmaatregelen op dit gebied genomen worden. Leveranciers melden dit uit gewoonte niet, of de functionaliteit is moeilijk te vinden in de documentatie zodat de klant/eindgebruiker niet weet wat hij feitelijk installeert.

TIP

In standaarden voor cybersecurity voor industriële besturingen (zoals WIB 2784, IEC 62443) wordt van leveranciers uitdrukkelijk geëist dat álle backdoors gemeld worden.

2.3.3 BEHEERDERSRECHTEN

Malware

Malware moet zichzelf, om een herstart van een PC (of waar het ook op draait) te kunnen overleven, ergens kunnen installeren. Dat zal veelal op de harde schijf zijn, maar elk opslagmedium is in principe goed: tegenwoordig USB-sticks, vroeger floppies en tapes. Door te voorkomen dat malware hierop zichzelf mag wegschrijven, is een infectie en/of overdracht al te voorkomen.

Het installeren van software is altijd toegestaan als de malware draait op zgn. "administrator" of "root" rechten. Indien dit niet het geval is, is installatie veelal direct

geblokkeerd (helaas niet in alle gevallen). Maar op veel systemen werken gebruikers altijd als beheerder, met als argument “dan kan ik alles”. Op zich klopt dat, maar de vraag is waarom gewone gebruikers zulke uitgebreide mogelijkheden op een PC moeten krijgen. Het laten werken van gebruikers met beperkte rechten (in elk geval geen rechten om software te installeren) is in zakelijke IT omgevingen zeer gebruikelijk. Het klopt dat soms de systeembeheerder om hulp gevraagd moet worden, maar dit is wel een zeer effectief filter op het ‘schoon’ houden van een PC en houdt tegelijk ook nog allerlei malware buiten de deur.

Malware

Erger is: software die alléén goed kan functioneren als het beheerdersrechten krijgt. Dit is een zeer gevaarlijke ontwerpfout in software, waarmee zeer voorzichtig omgegaan moet worden. In elk geval is een goed gesprek met de leverancier nodig, want het risico ligt dan bij u, niet bij de auteur van deze software.

ALARM

Wordt alle malware nu gestopt als een gebruiker geen beheerdersrechten heeft? Het antwoord hierop is: nee. Uiteraard weten hackers ook dat hun malware terecht kan komen in een gelimiteerde gebruikersomgeving. Malware zal dan proberen om misbruik te maken van bepaalde beveiligingslekken om zodoende alsnog (clandestien) beheerdersrechten te krijgen. Extra beveiligingsmaatregelen zijn dus nog gewenst.

2.4 ARCHITECTUURFOUTEN

Beveiligingslekken van deze orde ontstaan door misbruik te maken van de structuur van de software, of de omgeving waarin deze werkt. Het is eigenlijk niet persé een fout, maar eerder een manier van gebruik van de software die nooit voorzien was en waaraan ook weinig te doen is zonder de fundamenten ervan geheel opnieuw op te zetten.

BUG

De Amerikaanse "drones" die boven Iran vliegen zijn afhankelijk van GPS voor hun navigatie. Door nu zelf een vals GPS signaal uit te zenden met afwijkende coördinaten, denkt de drone dat hij ergens anders is en past zijn koers aan. Op deze manier kan de koers van de drone gewijzigd worden.

PRAKTIJKVOORBEELD

Een programma in C kan zichzelf of zijn geheugen overschrijven (tenzij verboden door de CPU zelf). Dat is een ideale omgeving voor malware, omdat de data waarop een programma werkt gewijzigd kan worden, of een programma ongezien gewijzigd kan worden door de malware. Het biedt eindeloze mogelijkheden voor malware auteurs. Een voorbeeld hiervan is: de "buffer overflow".

Programma's geschreven in de programmeertaal C, populair sinds de jaren 80, zijn ook vaak kwetsbaar. Aangezien C (en opvolger C++) nog steeds zeer populair zijn voor gebruik in operating systemen (zoals Windows, Linux), embedded software en industriële besturingen, PLC's en randapparatuur, is dit al twintig jaar een zeer actueel probleem. Een directe oplossing is niet voorhanden.

PRAKTIJKVOORBEELD

Microsoft zelf poogt zijn software op een speciale manier te ontwikkelen zodat beveiligingslekken van deze orde zoveel mogelijk worden uitgebannen. Verder zijn technieken zoals "DEP" (Data Execution Prevention) en "ASLR" (Address Space Layout Randomization) ontwikkeld om het moeilijker te maken Windows applicaties te hacken.

2.5 CONFIGURATIEFOUTEN

Zelfs als software foutloos is (een hypothetische aanname!) dan nog is het vaak mogelijk er misbruik van te maken, bijvoorbeeld omdat de gebruiker de software niet goed heeft geconfigureerd. Dit gebeurt vaak uit onwetendheid en soms

ook puur uit gemak. Hierover zijn tientallen voorbeelden te geven.

- Gebruik maken van eenvoudige, te korte, of te raden wachtwoorden;
- Firewalls die alle netwerkverkeer doorlaten; *Firewall*
- Mogelijkheid bieden om belangrijke bestanden te kunnen overschrijven;
- Virusscanners met verouderde configuratie;
- Toegang tot PC's mogelijk maken met verouderde protocollen;
- Draadloze netwerken zonder wachtwoord;
- Gebruik van beheerdersrechten voor dagelijkse werkzaamheden;
- Backdoors onterecht open laten staan; *Backdoor*
- Etc.

Vaak wordt alleen gedacht aan configuratiefouten op industriële PC's, maar ook alle gebruikte softwarepakketten, alle andere apparatuur, inclusief die op het netwerk, kunnen een verkeerde configuratie bevatten.

2.6 GEBRUIKERSFOUTEN

Onder deze categorie kunnen zeer veel soorten fouten verzameld worden; hackers maken er dankbaar gebruik van:

- Het ongewijzigd laten van fabriekswachtwoorden. Omdat het niet hebben van een wachtwoord op apparatuur tegenwoordig 'not done' is, wordt vaak "af fabriek" al een wachtwoord ingesteld. Omdat dit uiteraard voorspelbaar moet zijn, is het vaak altijd hetzelfde wachtwoord. Dit weten hackers ook en daarom moet het fabriekswachtwoord altijd meteen worden vervangen door iets anders.

- Ook al zijn de fabriekswachtwoorden gewijzigd, dan moet nog voorkomen worden dat ze ooit weer teruggezet worden. Bij de meeste merken apparatuur is het mogelijk om de fabrieksinstellingen terug te krijgen, bijvoorbeeld door het indrukken van een (reset)schakelaar

of een toetscombinatie. Gebruikersvriendelijk als dit moge zijn, vanuit het standpunt van cybersecurity is dit ongewenst: beveiligingsinstellingen zijn gewist en opeens mag iedereen alles, fabriekswachtwoorden zijn terug, filters worden gewist, netwerkpoorten kunnen weer opengezet zijn, etc.

Fysieke toegang tot zulke apparatuur moet dan ook voorkomen worden, bijvoorbeeld door de apparatuur in een afsluitbare ruimte te plaatsen.

- Het niet gebruik maken van de laatste versies van software, waarin alle bekende beveiligingslekken en achterdeurtjes opgelost zijn. Dit is een valkuil voor veel bedrijven.

- Gebrek aan kennis over de beveiligingsnoodzaak van systemen, waardoor deze vaak geheel onbeveiligd worden aangesloten. Dit is vooral te zien bij producten waar vaak "aansluiten en werken maar!" het credo is. Maar dit is vaak alleen mogelijk doordat alle beveiligingen 'af fabriek' uit staan. Dit maakt de inbedrijfname wel erg eenvoudig, maar vanwege onwetendheid met beveiligingsaspecten wordt de beveiliging dus ook niet ingeschakeld. Hoofdstuk 5 gaat hier dieper op in.

PRAKTIJKVOORBEELD

Een medewerker van een toeleverancier van Europol kopieert vertrouwelijke documenten op een "network attached storage" (NAS) server thuis. Dat merk heeft echter het wachtwoord standaard uitgeschakeld, zodat alle op die server opgeslagen documentatie via internet voor iedereen te lezen is.

2.7 OVERBELASTING

Door een processor te overbelasten, kan ervoor gezorgd worden dat software foutief gedrag gaat vertonen of geheel stopt met functioneren. Eén manier om dat te doen is om extreem veel CPU-capaciteit te gebruiken via lokale

malware. Deze vorm van misbuik is echter eenvoudig op te sporen en uit te schakelen.

Malware

Een moeilijker te bestrijden aanval is om extreem veel netwerkverkeer naar een bepaald systeem te sturen. Elk netwerkbericht moet immers bekeken worden door de lokale software; ook al wordt er verder niets mee gedaan, het kost uiteindelijk tóch CPU-capaciteit. En voor een hacker is het voordeel dat er op het aan te vallen systeem zelf niets gedaan hoeft te worden.

Met firewalls is ongewenst verkeer van buiten een bedrijf of een bepaald deel van een netwerk te blokkeren. Segmentering van een netwerk via routers blokkeert externe broadcasts; switches met "rate limiting" kunnen lokale broadcasts boven een bepaalde grens blokkeren.

TIP

Zo'n "Denial of Service" (DoS) aanval kan op elk apparaat met een netwerkaansluiting worden uitgevoerd. Een zorgvuldig ontwerp van de software op een apparaat kan de gevolgen van een DoS aanval sterk verminderen, bijvoorbeeld door op zijn minst niet te crashen – want dan functioneert het apparaat helemaal niet meer, waardoor het opnieuw opgestart moet worden.

Denial of Service

Wanneer er een DoS aanval wordt uitgevoerd op de PLC's van Phoenix Contact, is gedurende deze aanval de webserver van deze PLC tijdelijk niet bereikbaar maar blijven de vitale functies, zoals het besturingsprogramma gewoon functioneren.

PRAKTIJKVOORBEELD

2.8 WAT IS ER AAN TE DOEN?

Zoals in dit hoofdstuk genoemd is er een groot scala aan mogelijke foutenbronnen waar hackers gebruik van kunnen maken. Dit maakt het dan ook erg lastig om een systeem

waterdicht te beveiligen. En ook al is een systeem 100% veilig op de dag van oplevering, beveiligingslekken worden in de loop der jaren stuk voor stuk ontdekt, zodat dat systeem toch steeds kwetsbaarder wordt. Daarnaast zijn er nog de gebruikers- en configuratiefouten, die elke dag gemaakt worden door eigen personeel.

THINK

Het gevolg voor een beveiligingsbeleid is dat controles op alle gebieden nodig zijn én blijven. Standaarden voor cybersecurity (zoals IEC 62443, zie hoofdstuk 7) eisen dan ook dat processen en procedures op dit gebied ingericht worden.

TIP

Firewalls en virusscanners die niet 'up to date' worden gehouden met maatregelen tegen actuele dreigingen, hebben geen zin. Hiermee worden ze zelf kwetsbaar voor hackers. Leveranciers van virusscanners bieden hiervoor abonnementen aan. Omdat een firewall de eerste verdedigingslinie van een bedrijf of systeem is, is het uitermate belangrijk de status ervan goed te monitoren!

HOOFDSTUK 3

IT EN IT

3. IT EN IT

Wie bekend is met zowel de “zakelijke / bestuurlijke IT” als de “industriële IT” valt het meteen op: dit zijn twee verschillende werelden, ook al is de afkorting “IT” hetzelfde. Maar daar houden de overeenkomsten ook grotendeels op. Zoals hieronder in meer detail besproken wordt, zijn er veel verschillen: de applicaties, de gebruikte apparatuur, de gebruikte software, soort personeel en hun opleiding en kennis, levensduur van systemen, eisen aan beschikbaarheid, werkprocedures, innovatie, etc. Deze verschillen hebben ook hun consequenties voor de aanpak van de beveiliging.

In de eerste plaats wordt de noodzaak tot het hebben van een voldoende beveiliging in de industriële IT nog maar zelden onderkend; “wij worden niet gehackt” (hoofdstuk 5 gaat dieper op dit soort misvattingen in). Deze opvatting is niet geheel onterecht, want er is nog maar vrij weinig gebeurd maar dat is snel aan het wijzigen *(zie hoofdstuk 4*). En voor wie cybersecurity wel serieus neemt: de in de zakelijke IT gangbare beveiligingsprocedures zijn vaak in de industriële IT geheel of grotendeels onbruikbaar. Daarom zijn er sinds twee jaar ook specifieke beveiligingsnormen op industrieel gebied, zoals de ISA-99 / IEC 62443 en de WIB-standaard (in hoofdstuk 7 meer in detail besproken).

IEC 62443

SCADA

Pas sinds enkele jaren is er meer belangstelling voor de cybersecurity van de industriële IT. De hierin gebruikte hardware en software wordt vrij consequent met de verzamelnaam "SCADA" aangeduid. Dit is op zich natuurlijk niet terecht want SCADA-systemen zijn maar één van de vele soorten hardware en software die in de industriële IT gebruikt worden.

3.1 VERSCHILLEN IN BESCHIKBAARHEID, INTEGRITEIT EN BETROUWBAARHEID

De Engelse woorden "confidentiality" (C), "integrity" (I) en "availability" (A) worden vaak gebruikt in deze volgorde (CIA) om binnen de zakelijke IT de prioriteiten aan te geven: bescherming van data heeft de hoogste prioriteit en de beschikbaarheid van de IT-systemen is minder belangrijk. Niet dat het dan geheel onbelangrijk is maar de meeste bedrijven hebben er geen last van als na werktijd of in het weekend de IT-systemen niet beschikbaar zijn.

In de industriële IT worden de prioriteiten anders gesteld (AIC): beschikbaarheid van productiemiddelen heeft de allerhoogste prioriteit, hier wordt immers het geld verdiend, of uitval is maatschappelijk problematisch (bijvoorbeeld waterwinning, energiecentrales, etc.). Daarna volgt integriteit en als laatste betrouwbaarheid (uiteraard is het vervelend als productiegegevens, recepten, programma's e.d. op straat komen te liggen). Sommigen stellen dat vóór beschikbaarheid nog een andere, véél belangrijkere prioriteit, moet komen: "safety" (veiligheid) van personeel en de maatschappij.

De beschikbaarheid van een industriële toepassing wordt geheel anders bepaald dan in een zakelijke omgeving. Is op een kantoor één PC niet meer functioneel, dan kunnen alle andere collega's nog gewoon doorwerken. Maar in een productieomgeving moet alle apparatuur goed functioneren: uitval van één PLC of een I/O module maakt dat een gehele productielijn niet meer kan werken. Immers, alle apparatuur werkt met elkaar samen. In een kantooromgeving werken de PC's afzonderlijk van elkaar, uiteraard op dezelfde infra-

structuur en op dezelfde data(bases), maar wel afzonderlijk van elkaar. Dit ogenschijnlijk eenvoudige verschil (CIA versus AIC) heeft belangrijke consequenties voor de werkwijze rondom cybersecurity. Waar in de zakelijke IT een systeembeheerder nog wel kan zeggen "dit weekend gaat het netwerk uit de lucht voor onderhoud" is dit in veel industriële omgevingen absoluut onmogelijk; soms is er enkel tijd tijdens de tweejaarlijkse productiestop of in een vakantieperiode.

Patchen

Dit houdt dan ook in dat er op systemen geen nieuwe software geïnstalleerd ("patchen") kan worden om bekende beveiligingslekken te dichten, dat systemen niet opnieuw gestart ("reboot") mogen worden, dat geen systeemdelen vervangen kunnen worden of uitbreidingen kunnen worden aangekoppeld, etc.

Penetratietest

Ook (strenge) eisen op het vlak van safety werken door in de cybersecurity. Een "penetratietest" die door een (veelal externe) expert wordt uitgevoerd om te zien of in een netwerk ingebroken kan worden, kan voor uitval van een industriële besturing zorgen, zeker als het om oudere apparatuur gaat.

Firewall

Anderzijds is het echter ook ongewenst als bekende beveiligingsproblemen maanden of jarenlang niet aangepakt kunnen worden. Hiervoor zijn ook wel weer oplossingen in de markt aanwezig (bijvoorbeeld "virtual patching" op firewalls), maar daar moet dus wel rekening mee gehouden worden in het pakket van eisen. De processen en procedures voor configureren, installeren, wijzigen, testen en patchen van software zijn in een industriële IT-omgeving ook anders dan in de zakelijke IT. Netwerk- en systeembeheerders realiseren zich dit niet altijd en dit levert vaak de nodige frictie op - de beheerders worden door de organisatie verantwoordelijk gesteld voor het adequaat beveiligen van de (zakelijke en industriële) IT systemen, maar het productiemanagement zal alle noodzakelijke werkzaamheden ondergeschikt maken aan de productiedoelstellingen. De verschillen tussen de zakelijke en industriële IT maken dat bestaande standaarden voor

cybersecurity, zoals ISO 2700X, veel onderdelen bevatten die voor de industrie óf geheel niet van toepassing zijn, of anders ingevuld moeten worden. Er zijn dan ook speciale standaarden ontwikkeld specifiek voor de industriële IT *(zie hoofdstuk 7)*.

3.2 TECHNISCHE VERSCHILLEN

Naast verschillen in processen, procedures en prioriteiten zijn er ook nog de nodige technische verschillen tussen de zakelijke en industriële IT. De onderstaande tabel somt er een aantal op.

Aspect	Zakelijke IT	Industriële IT	Consequentie
Netwerk-technologie	Ethernet	Ethernet op hogere niveaus; veldbussen op laagste niveaus	Toenemende kwetsbaarheid, doordat Ethernet gebaseerde systemen steeds meer worden toegepast in de industrie
Draadloze netwerken	WiFi	WiFi, Bluetooth, ISA-100, Wireless-HART	Toenemende kwetsbaarheid, doordat WiFi steeds meer wordt toegepast in de industrie
Protocollen	TCP/IP familie	TCP/IP, industrieel Ethernet, veldbussen	Verschillende technologieën
Bandbreedte Ethernet	Gbit/s	100 Mbit/s voor besturingstoepassingen	-
Realtime eisen	Geen	Hoog	Externe beïnvloeding is ongewenst
Netwerkbelasting	Zeer variabel	Zeer voorspelbaar en constant	Maakt detectie van malware eenvoudiger

Aspect	Zakelijke IT	Industriële IT	Consequentie
Redundantie	In grotere organisaties, via standaard protocollen hiervoor (STP b.v.)	Zelden beschikbaar voor veldbussen; voor industrieel Ethernet via leverancierspecifieke protocollen; op hoger niveau via bijvoorbeeld MRP	-
Type switch	Altijd managed switches	Nog veel unmanaged switches	Unmanaged Switches bieden geen netwerk monitoring en diagnose
Leverancier netwerk apparatuur	Cisco, HP, etc.	Vaak dezelfde als besturingsleverancier	-
Onderhoud aan netwerk	Na kantooruren, in weekend	Alleen mogelijk tijdens productiestop	Uitbreidingen / wijzigingen maar langzaam door te voeren
Consequentie uitval individuele PC	Geen directe consequenties voor organisatie	Leidt veelal tot productiestop (“Loss of view, loss of control”)	Afzonderlijke update / herstart is niet mogelijk
Gebruik TCP/IP adressen	Via DHCP, welk IP adres maakt niet uit	Vaak nog via statische IP adressen	Ontbreken van een DHCP server is een kwetsbaarheid minder, maar een IP-adres dubbel gebruiken is vaak fataal (gevaar van handmatige administratie)

Aspect	Zakelijke IT	Industriële IT	Consequentie
Soort apparatuur	PC, printer, file/ e-mail server, internet proxy, database	PLC, DCS, SCADA/ HMI, PC, remote I/O, vision, frequentie omvormers / motion, sensoren	Grote variatie in apparatuur vereist veel maatwerk
Locatie apparatuur	Bureaus, serverruimte, schakelruimte; vrij gecentraliseerd	Operator ruimte, bij machines / productielijn, zeer verspreid	Fysieke toegangscontrole tot netwerk en apparatuur moelijker af te dwingen
Toegang tot apparatuur	Alleen voor beheerders via afgesloten ruimtes	Veelal voor iedereen in productie mogelijk	Fysieke toegangscontrole is niet altijd mogelijk
Levensduur systeem	5 jaar	15...20 jaar	Verouderde hardware en software met oude kwetsbaarheden
Programmeertalen	C / C++, Java, Flash, Perl, Ruby, Python, Lua, PHP, SQL, e.v.a.	IEC-61131, C / C++, veel leverancierspecifieke omgevingen	Minder aandacht van hackers
Operating systems	Windows, Linux	Veel leverancierspecifieke omgevingen, Windows, VxWorks, Linux, Windows Embedded	Grote variatie in software vereist veel maatwerk
Type PC	Desktop, laptop	Industriële variant voor besturing, anders redelijk standaard PC. Laptop voor configuratie, diagnose	Laptops van toeleveranciers vallen buiten eigen beveiligingsmaatregelen

Aspect	Zakelijke IT	Industriële IT	Consequentie
Windows versie	recent (Windows7, Windows8)	Vaak nog XP of NT	Geen patches tegen actuele beveiligingsproblemen beschikbaar vanuit Microsoft
Beheer van PC	Systeembeheerder	Vaak productiepersoneel	Ondergeschikt aan productie-eisen
Virusscanner op PC	Ja	Zelden	Geen bescherming tegen bekende veiligheidsproblemen
Ophalen van patches	Rechtstreeks via internet bij leverancier	Handmatig bij leverancier; vaak geen internettoegang of kan niet automatisch	Meer handwerk nodig, tijdrovender waardoor minder "up to date"
Patch frequentie	Met maandelijkse Microsoft cyclus	Veelal geen; soms tijdens productiestop	Zeer lange periode van kwetsbaarheid
Testen van patches	Wordt vertrouwd op leverancier	Is nodig vóór installatie op productiesystemen	Patches niet automatisch laten installeren
Software updates	Frequent	Alleen indien nodig	Vaak zeer verouderde software in gebruik
Herstart van systeem	Dagelijks / wekelijks / na patch	Zelden	Patches, ook al zijn ze geïnstalleerd, worden niet geactiveerd

Aspect	Zakelijke IT	Industriële IT	Consequentie
Wachtwoorden	Verplicht	Geen, of aan iedereen bekend, geen wijziging na ontslag / vertrek medewerker	Laag niveau van beveiliging
Account lockout na teveel foute inlogpogingen	Ja	Nooit	Lockout zou toegang / beheer systeem onmogelijk maken
Wachtwoord-wijziging	Regelmatig	Nooit	Wachtwoorden zijn jarenlang hetzelfde
Securitybewustzijn	Continu	Bij aanschaf en inbedrijfname	Verouderde technologie niet opgewassen tegen moderne bedreigingen

Industriële PC's zijn in principe gewone PC's, maar aangepast aan de specifieke omgeving waarin ze moeten werken (temperatuurbereik, trillingen, EMC, etc.). Qua software wordt veelal gebruik gemaakt van Windows. Maar omdat de levensduur van industriële PC's véél langer is dan de gemiddelde PC op kantoor, is de versie van Windows die gebruikt wordt slechts zelden de recentste. Dat is technisch geen probleem, immers de applicatiesoftware is juist gemaakt voor die versie. Maar Microsoft voert geen onderhoud uit aan Windows-versies waarvan de levensduur (volgens Microsoft) verstreken is, er komen dus ook geen "security hotfixes" meer uit voor ontdekte beveiligingslekken in Windows XP SP1, SP2 en SP3, Windows 2000, NT, 99 en 95.

Virusscanner

Soms wordt aangenomen dat een virusscanner op die oude Windows versies de bescherming tegen malware in stand houdt. Echter oude virusscanners worden veelal niet meer onderhouden door de respectievelijke leveranciers; ze beschermen dus alleen tegen oude malware en niet meer tegen de nieuwste.

HOOFDSTUK 4

INCIDENTEN

4. INCIDENTEN

De afgelopen jaren zijn er veel incidenten geweest met slecht beveiligde IT-systemen, ook in de industrie. In dit hoofdstuk zullen we er enkele bespreken. Dat wil niet zeggen dat er verder niets gebeurd is; wie het in de gaten houdt zal opvallen dat er in de pers (krant, websites, TV) nog best wel regelmatig incidenten voorbijkomen die gerelateerd zijn aan falende cybersecurity.

Virus

Enkele voorbeelden: de inbraak bij certificatenleverancier DigiNotar (dat hierdoor ook failliet ging), het virus dat een ziekenhuis platlegde, het uitlekken van de kersttoespraak van het Nederlandse koningshuis in 2011, 2012 én 2013, inbraken in de websites van diverse grote en kleine bedrijven (KPN, Belgacom, Philips, etc.), de zwakke beveiliging van het WiFi-systeem van de Thalys-trein, de inbraak in het videoconferencing systeem van het Nederlandse ministerie van Defensie, de overnames van het gebouwbeheersysteem van een sporthal en van een zwembad, de zwakke beveiliging in honderdduizenden (consumenten-) routers, printers, NAS-servers enz. Dit staat dan nog los van alle incidenten rondom gijzelvirussen, phishing-mails, telefoontjes van nep Microsoft medewerkers, geplunderde bankrekeningen, etc. In 2013 kwam daar nog bij dat de Engelse veiligheidsdiensten actief waren in het netwerk van Belgacom en samen met de Amerikanen massaal telefoons afluisterden, op laptops microfoons en webcam's activeerden, routers manipuleerden, in reserveringssystemen van tophotels meekeken, besmette USB-sticks aan diplomaten uitdeelden, etc.

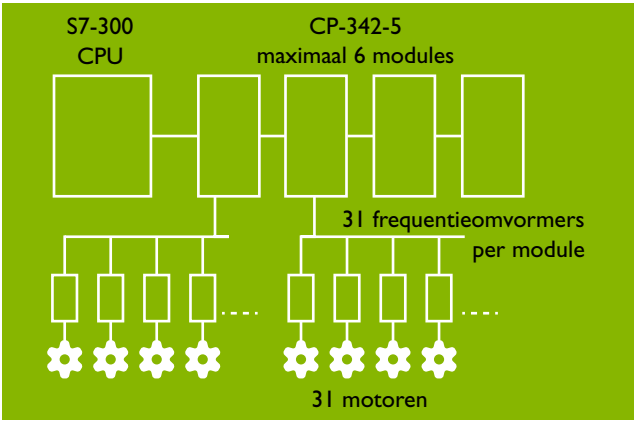
En dat zijn dan nog maar de incidenten die bekend werden; waarschijnlijk is het nog maar het topje van de ijsberg. Veel bedrijven lijken zich erg te schamen om genoemd te worden als doelwit van een 'hack' en als men toch genoemd wordt zal gepoogd worden het incident zoveel mogelijk dood te zwijgen. De ruimte ontbreekt om alle incidenten in detail te beschrijven. Daarom beperken we ons tot enkele spraakmakende 'hacks' op industriële systemen.

4.1 INCIDENT I

Het meest spraakmakende incident van de afgelopen jaren waarbij een industriële besturing betrokken was vond plaats in Iran. In de zomer van 2010 ontdekte een beveiligingsbedrijf dat er een onbekend virus intern rondwaarde. Na een eerste analyse bleek er iets vreemd aan de hand: het virus leek helemaal niets te doen, anders dan zichzelf voort te planten. Maar een diepere analyse bracht aan het licht dat het virus, inmiddels Stuxnet genaamd, op zoek was naar een database van het Siemens' Step7 engineeringtool. Dit was de eerste indicatie dat het hier om een geheel nieuw type virus ging. Na deze melding gingen meer bedrijven wereldwijd zich met de analyse van Stuxnet bezighouden. De omvang en de complexiteit van Stuxnet maakten dat het meer dan een half jaar duurde voordat de complete werking ontcijferd was. Zelfs in 2013 kwamen met enige regelmaat nog steeds nieuwe onthullingen over Stuxnet.

Virus

Stuxnet



Opbouw van het door Stuxnet aangevallen systeem *(bron: Symantec)*

Virus

Stuxnet bleek een virus te zijn speciaal gemaakt om één industrieel systeem in de wereld aan te vallen. Het systeem zou bestaan uit een flink aantal Siemens S7 PLC's, met Profibus/DP gekoppeld aan tientallen frequentieomvormers van twee merken, waarmee motoren met extreem hoge toerentallen aangestuurd zouden worden. Al snel was duidelijk dat er maar één soort fabriek zo opgebouwd is: een uraniumverrijkingsplant. Daarvan bestaan er maar weinig

in de wereld (oa. Urenco in Almelo). De consensus onder experts is dat Stuxnet speciaal bedoeld was voor het vernietigen van de Iraanse opwerkingsplant in Natanz, om zodoende de Iraanse nucleaire ambities te dwarsbomen of in elk geval te vertragen. Alhoewel dat door Iran ontkend wordt, lijkt Stuxnet wel succes gehad te hebben.

Stuxnet

◀ De Iraanse president loopt door de opwerkingsfabriek *(bron: www.president.ir)*

De werking van Stuxnet is bijzonder, omdat dit het eerste virus is dat ook speciaal gemaakt is voor een PLC. Uiteraard maakte het gebruik van beveiligingslekken in Windows om binnen te dringen en zich te verspreiden. De Step7 database was toegankelijk omdat het wachtwoord hiervan overal ter wereld hetzelfde is en al jaren circuleerde op internet. Stuxnet zocht in de Step7 database naar één bepaald PLC-programma; vond het dit niet dan bleef het virus verder inactief. Vond het dat ene gewenste PLC-programma wél, dan werd het gemodificeerd en bij de eerstvolgende gelegenheid op de PLC geladen. Na activatie op de PLC werd gedurende enige tijd de werking van de opwerkingsfabriek gevolgd. Op een bepaald moment begon het virus de frequentieomvormers zodanig om te programmeren dat de hieraan gekoppelde ultracentrifuges op te hoge toerentallen zouden gaan draaien, met als resultaat dat deze uit elkaar zouden spatten. Hierdoor zou ook het giftige en radioactief uraniumhexafluoridegas zich in de fabriek gaan verspreiden. In elk geval, de productie van verrijkt uranium zou moeten stoppen.

Virus

Om geen argwaan bij de operators te veroorzaken, werden deze misleid met valide operationele data op hun consoles. Deze gegevens had Stuxnet eerder verzameld.

Het is duidelijk dat Stuxnet niet door een paar hackers thuis gemaakt is. Geschat wordt dat de ontwikkeling ervan enkele miljoenen dollars heeft gekost. Er wordt zelfs gedacht dat er een deel van een opwerkingsfabriek is nagebouwd om de software van het virus te testen. Een eerste versie van Stuxnet had niet het verwachte effect, daarom is later een tweede versie gemaakt. Wie er achter zit, daarover wordt genoeg gespeculeerd - waarschijnlijk politieke tegenstanders van Iran.

Virus

Cyberwar

ALARM

De consequenties van Stuxnet buiten Iran zijn onbekend, mogelijk is er geen directe schade aangericht omdat het virus nergens de juiste systeemconfiguratie vond. Dat wil niet zeggen dat er geen systemen besmet zijn geraakt; volgens Symantec zijn er 150 besmettingen in Nederland gedetecteerd.

4.2 INCIDENT 2

Begin 2012 publiceerde een Nederlandse hacker een lijst van industriële systemen die hij via internet kon benaderen. Deze waren gevonden via de zoekmachine Shodan, die ontwikkeld is om te zoeken naar apparatuur die op internet is aangesloten (net zoals Google zoekt naar documenten, foto's en films, *zie ook hoofdstuk 5*). Hij nam contact op met de overheid, maar vond daar volgens eigen zeggen geen gehoor en plaatste vervolgens de lijst op internet. Op de lijst kwamen, naast veel buitenlandse systemen, ook systemen van gerenommeerde Nederlandse bedrijven voor.

Het webzine Webwereld, welke door de hacker was ingelicht, publiceerde daarna over het totale gebrek aan beveiliging van het beheerssysteem van een sporthal. Zonder gebruikersnaam en zonder wachtwoord kon iedereen de verwarming hoger of lager zetten, de instellingen van de

airconditioning aanpassen, het alarmsysteem aanpassen en logboeken lezen.

Een maand later kwam Webwereld nogmaals met een publicatie over een slecht beveiligd via internet toegankelijk besturingssysteem, ditmaal van een subtropisch zwembad. De temperatuur van het water en de attracties konden op afstand worden gewijzigd. In eerste instantie werd alarm geslagen omdat het leek alsof de chloortoediening ook gewijzigd kon worden (maar dat bleek later niet het geval).

Volgens de systeemintegrator die de technische installatie heeft aangeleverd was het wel mogelijk om de communicatie via internet te beveiligen, maar had de klant hiervoor niet gekozen, omdat een inbraak via internet niet als risico werd gezien.

THINK

4.3 INCIDENT 3

Een poging om bij het Nederlandse chemiebedrijf DSM in te breken vond plaats in de zomer van 2012. Een medewerker vond 's ochtends op de personeelsparkeerplaats een USB-stick. In plaats van toe te geven aan de neiging om deze USB-stick in de eigen PC te bekijken, ging de vinder eerst naar de IT-afdeling om de stick te laten scannen op malware. Er bleek inderdaad een virus op te staan. Daarna is de parkeerplaats verder nagezocht en zijn nog meer besmette USB-sticks aangetroffen.

Malware
Virus

Door de juiste actie van de medewerker is verdere besmetting van het bedrijf voorkomen.

CHAPEAU

4.4 INCIDENT 4

Virus

Ook in de zomer van 2012 werd Saudi Aramco in Saudi-Arabië getroffen door het blijkbaar speciaal voor dit bedrijf ontwikkelde virus genaamd "Shamoon". Een hackersgroep genaamd "Swords of Justice" claimde dat het dit virus ontwikkeld had. Op het moment van ontdekking waren al 30000 PC's van Aramco geïnfecteerd. Al deze PC's waren geprogrammeerd om op 15 augustus (een vakantiedag) te beginnen met het overschrijven van alle documenten en afbeeldingen door een foto van een brandende Amerikaanse vlag. Er waren geen productiesystemen getroffen door het virus. Door de tijdige ontdekking was het mogelijk om tegenmaatregelen te nemen; daarna waren nog drie weken nodig om alle PC's op te schonen.

Beveiligingsbedrijf WebSense kwam later met de mededeling dat hun eigen beveiligingssoftware een deel van Shamoon eind 2010 al gedetecteerd had. Dit suggereerde dat het infectieproces al langer liep; mogelijk waren de auteurs hun software aan het testen.

4.5 INCIDENT 5

Met de zoekmachine "Shodan" (waarmee eenvoudig naar apparatuur gezocht kan worden die op internet is aangesloten) is het erg eenvoudig geworden om te zoeken naar bepaalde merken apparatuur. De Nederlandse beveiligingsexpert Oscar Kouroo ontdekte op deze manier dat veel Nederlandse apparatuur zonder adequate beveiliging aan internet was gekoppeld. Hierover maakte het TV-programma "EenVandaag" een reportage.

Het wachtwoord van de apparatuur voor de gemeente Veere bleek zeer eenvoudig te raden. Daardoor konden rioleringspompen en gemalen op afstand bediend worden. Verder werd ook genoemd dat uitwateringssluizen op afstand te bedienen waren. In de reportage komt ook aan de orde wat de gevaren zouden kunnen zijn voor de stabiliteit van een zeedijk.

De besturing van de sluizen in Veere werd door het TV-programma niet overgenomen. Om toch aan het publiek de mogelijkheden van een digitale inbraak te tonen, is op afstand de centrale verwarming van het hoofdkantoor van het Leger des Heils uitgezet. In de reportage is een personeelslid te zien die meldt “nu is het duidelijk waarom het hier vorige week zo koud was”. In de reportage kwam één merk apparatuur duidelijk in beeld, maar dit had verder niets met de kwetsbaarheden te maken.

4.6 INCIDENT 6

Criminelen hadden dankzij hackers toegang gekregen tot de administratieve database van een containeroverslagbedrijf in Antwerpen. Hierdoor konden zij containers (met drugs) volgen die vanuit Zuid-Amerika naar Europa verscheept werden. Eenmaal aangekomen in de haven konden de containers op een bepaalde plaats worden neergezet, zodat ze snel met een vrachtwagen konden worden opgehaald vóórdat de echte eigenaar er was.

Keyloggers

De criminelen volgden de containers via de computersystemen van het overslagbedrijf. Enkele belangrijke computersystemen waren voorzien van keyloggers, die tijdens een inbraak waren aangebracht. Hiermee kon elke toetsaanslag op afstand worden uitgelezen; tevens werden regelmatig screendumps gemaakt. De verzamelde data werd via een internetverbinding naar een externe server gestuurd.

Een firewall kan ook ingesteld worden om uitgaand verkeer te blokkeren: alle netwerkverkeer, of alleen netwerkverkeer afkomstig vanaf bepaalde systemen, of gericht op bepaalde externe systemen, of alleen bepaalde protocollen, etc.

THINK

HOOFDSTUK 5

MISVATTINGEN

5. MISVATTINGEN

Eén van de redenen waarom er vaak zo weinig gedaan wordt aan het cyberveilig maken én houden van industriële systemen is dat men zich niet kwetsbaar voelt en de risico's dus niet ziet. Een aantal misvattingen zijn hier de oorzaak van. Enkele voorbeelden:

- "Er zit een wachtwoord op";
- "Ik heb een virusscanner";
- "Niemand heeft interesse in mij";
- "Ik hang niet aan internet";
- "Het heeft geen zin, ze komen er toch doorheen";
- "Ik gebruik geen Windows";
- "Hackers komen enkel van buiten".

In de volgende paragrafen gaan we dieper in op deze misvattingen.

5.1 MISVATTING: ER ZIT EEN WACHTWOORD OP

Het gebruik van een wachtwoord is een van de meest voorkomende beveiligingsmaatregelen. Maar het ene wachtwoord is het andere niet.

Simpele wachtwoorden als "geheim" en "123456" zijn uiteraard compleet nutteloos. Niemand gebruikt in deze tijd zo'n wachtwoord, toch? Uit onderzoek blijkt het tegenovergestelde: het zijn de twee meest gebruikte wachtwoorden. Een hacker die de top-20 aan wachtwoorden probeert heeft in veel gevallen al direct prijs.

Een tweede categorie wachtwoorden die niet meer zouden moeten bestaan zijn fabriekswachtwoorden, die dus door een fabriek op elk nieuw apparaat worden ingesteld. De gebruiker van zo'n apparaat moet het fabriekswachtwoord direct na aanschaf wijzigingen in iets anders. Dit wordt vaak vergeten. Het eerste wat een hacker probeert om in een apparaat binnen te komen is: via het fabriekswachtwoord.

WEBSITE

Op internet is veel informatie te vinden over welke leverancier welk fabriekswachtwoord gebruikt; zie bijvoorbeeld: www.cirt.net/passwords

Een derde categorie wachtwoorden die ongebruikt zouden moeten blijven zijn te korte wachtwoorden. Wie een wachtwoord van één letter of cijfer gebruikt, heeft slechts 26+26+10 = 62 mogelijkheden. Daar draait een hacker zijn hand niet voor om, een klein programmaatje heeft alle mogelijkheden zo nagezocht. Twee karakters dan? Dat is 62*62 = 3844 mogelijkheden, nog zo na te zoeken. Met vijf karakters zijn al 916 miljoen wachtwoorden te vormen, met tien karakters al 839 biljard. Wie ook nog de andere karakters van het toetsenbord gebruikt, zoals \|`~!@#$%^&*()-_=+[{]}\|'";:.>,</? heeft per karakterpositie geen 62 maar 96 mogelijkheden en dan zijn er met vijf karakters 8,1 miljard wachtwoorden mogelijk en met 10 karakters 66 triljard. Dit is de reden dat langere wachtwoorden beter zijn dan kortere.

Brute force

Hackers laten zich door wachtwoorden niet afschrikken, integendeel - ze proberen ze gewoon allemaal uit. Gewoon beginnen bij aaaab, dan aaaac, etc. tot aaaaz, aaaba,aaabb, ..., zzzzx, zzzzy, zzzzz en dan verder met 6 letters, 7 letters, etc. Dit heet een "brute force" aanval. Uiteraard kost dit de nodige rekentijd en als een wachtwoord maar lang genoeg is wordt de rekentijd te lang om nog nuttig te zijn. De vraag is dus, hoeveel wachtwoorden kan een hacker in redelijke tijd uitproberen? Dankzij de aanwezigheid van moderne PC's is rekenkracht goedkoop te krijgen en dan heeft men nog maar één processor. Nog beter is het gebruik van een high-end grafische kaart, waarop tot enkele honderden processoren aanwezig zijn.

Dit geeft een enorme versnelling in het doorrekenen van mogelijke wachtwoorden; van enkele honderden pogingen per seconde tot meer dan honderdduizend. Dit aantal kan met meerdere grafische kaarten per PC en meerdere PC's nog aanzienlijk verhoogd worden en dat voor een investering van slechts een paar honderd Euro.

Een andere manier om wachtwoorden te kraken is het gebruik maken van wiskundige methodes. Een encryptiemethode kan namelijk een zwakte hebben, waardoor met wiskundige trucs wachtwoorden niet stuk voor stuk geprobeerd hoeven te worden, maar teruggerekend kunnen worden. Dit is zo gebeurd bij het "WEP" (Wired Equivalent Privacy) algoritme van draadloos Ethernet (WiFi). Waar in het begin een hacker nog enkele tientallen miljoenen netwerkberichten nodig had om een wachtwoord terug te rekenen, kan het tegenwoordig met maar een paar honderd netwerkberichten en is de rekentijd minder dan een seconde. Dit is de reden dat WEP vervangen is door opvolger WPA2. De tijd om een WPA2-wachtwoord terug te rekenen is nu nog enkele honderden malen de levensduur van het heelal, dus WPA2 is veilig (nog wel).

WEP

WPA2

Een vierde categorie wachtwoorden die niet gebruikt zou moeten worden: alles wat in het woordenboek staat, automerken, meisjesnamen, namen van voetbalclubs, al dan niet gevolgd door een of meer cijfers, normaal of achterstevoren geschreven, etc.. In tegenstelling tot een aanval die alle mogelijke combinaties van letters uitprobeert, heeft een taal veel minder woorden, merken en namen. Het "Dikke van Dale" woordenboek bevat 'maar' een kwart miljoen woorden. Deze zijn met een brute force aanval snel door te rekenen.

Brute force

De laatste categorie wachtwoorden die niet gebruikt zouden mogen worden: wachtwoorden die dezelfde gebruiker elders ook al heeft gebruikt (bijvoorbeeld op sociale media websites, webwinkels, etc.). Als dit gekoppeld kan worden aan een bepaalde gebruiker, dan kan een hacker dat wachtwoord elders ook gewoon als eerste proberen, met een

PRAKTIJKVOORBEELD

In 2012 kwam een wachtwoordenbestand van Philips werknemers in handen van hackers. Men nam aan dat, omdat Philips een Nederlands bedrijf is, de werknemers geneigd zouden zijn Nederlandse woorden als wachtwoord te gebruiken. Dit bleek met behulp van een bestand met veelgebruikte Nederlandse woorden in een kwart van de wachtwoorden te kloppen; er was slechts 3 seconde rekentijd voor nodig om hier achter te komen.

TIP

Een "wachtzin" is een methode om eenvoudig een lang wachtwoord te onthouden. Bijvoorbeeld, neem de zin: "De Kerstman woont op de Noordpool met zijn 4 rendieren". Neem dan steeds het eerste karakter, dit geeft het wachtwoord: DKwodNmz4r. Dit wachtwoord voldoet aan veel eisen: lang genoeg, niet in een woordenboek terug te vinden, geen fabriekswachtwoord, niet enkel letters en (vooral!) eenvoudig te onthouden.

redelijke kans op succes. Alhoewel dit op het eerste gezicht een probleem van die gebruiker zelf lijkt, kan een koppeling naar zijn werkgever soms snel gemaakt worden: bijvoorbeeld via LinkedIn.

5.2 MISVATTING: IK HEB EEN VIRUSSCANNER

Virusscanner

Een virusscanner is één van de meest bekende maatregelen die men kan nemen om virussen op een PC op afstand te houden. Dit komt omdat de noodzaak van het moeten hebben van een virusscanner op een PC eigenlijk bij iedereen wel bekend is.

Minder bekend is dat een virusscanner dagelijks (of liefst nog vaker) bijgewerkt moet worden om op de hoogte te zijn van de allernieuwste virussen. Deze dienst wordt vaak in de vorm van een abonnement verkocht; de leverancier houdt een database bij met virusdefinities en betalende klanten kunnen die via internet actualiseren. Is het abonnement verlopen, dan zal de virusscanner gaan achterlopen en de allernieuwste virussen niet meer herkennen.

Nog minder bekend is dat er grote verschillen zijn tussen virusscanners onderling in kwaliteit van detectie van de meest recent ontdekte virussen, processorbelasting, aantal onterechte meldingen, etc.

Het Oostenrijkse www.av-comparatives.org publiceert regelmatig vergelijkende onderzoeken naar de kwaliteiten van een twintigtal merken virusscanners. Opvallend hierbij is dat zelfs virusscanners van naam & faam 5% van alle virussen niet detecteren.

TIP

Om virusscanners goed hun werk te kunnen laten doen, moet hun configuratie over actuele malware actueel gehouden worden. Nieuwe configuratiegegevens worden door de leverancier gemaakt en moeten via internet opgehaald worden. Echter: het hebben van een internetkoppeling in een industriële toepassing geeft weer andere risico's. Maar een virusscanner die niet actueel blijft, heeft ook geen zin.

Virusscanner

De auteur controleert een PC vanwege de klacht "het is zo langzaam". Na controle blijken er maar liefst 3 virusscanners op te staan. Eén is om onduidelijke reden uitgeschakeld. Van de tweede is het abonnement verlopen en al jaren niet meer voorzien van nieuwe virusdefinities. De derde virusscanner lijkt beschadigd te zijn en doet het ook niet meer.

PRAKTIJKVOORBEELD

Soms zijn virusscanners erger dan de kwaal die ze bestrijden. In 2012 en in de eerste helft van 2013 is het driemaal voorgekomen dat vanwege een programmeerfout in een virusscanner (van 3 verschillende merken) PC's compleet geblokkeerd werden. Dit is uiteraard niet acceptabel voor een industrieel systeem, juist omdat virusscanners dagelijks automatisch bijgewerkt worden en men als gebruiker dus opeens geconfronteerd kan worden met een PC die geen

netwerkverbinding meer heeft en/of applicaties niet meer kan starten.

Gegeven deze zwakheden van virusscanners geven ze dus geen 100% waterdichte beveiliging tegen virussen en kunnen soms zelf een bron van uitval van apparatuur zijn. Andere maatregelen zijn dus ook nog nodig; een virusscanner is maar één schakel in de zgn. "defense in depth" strategie.

Virusscanner
Defense in depth

ALARM

Virusscanners worden vaak uitgeschakeld door gebruikers omdat de virusscanner de schuld krijgt van de 'traagheid' van de PC en/of het netwerk.

5.3 MISVATTING: NIEMAND HEEFT INTERESSE IN MIJ

Net zoals bij de gewone criminaliteit gaan velen er van uit dat cybercriminaliteit alleen anderen overkomt: "ik ben niet interessant", "bij mij is niets te halen". Maar afpersers denken hier anders over en concurrenten mogelijk ook.

Sinds de opkomst van internet en van draadloze netwerken is het erg eenvoudig om een persoon of bedrijf te vinden op internet. In de eerste plaats zijn cybercriminelen continu bezig om internet af te scannen op basis van IP-adressen, puur om te zien of er "iets" is. Dit doet men eenvoudigweg door een "ping" commando te sturen; is er niemand dan komt er geen antwoord en zoekt men verder.

Ping

THINK

Vanwege de omvang van internet kostte het tot 2012 nog meerdere maanden om alle mogelijke IP-adressen uit te proberen. In 2013 kwam de universiteit van Michigan met een nieuwe zoekstrategie waarmee alle IP-adressen binnen drie kwartier al af te vragen zijn.

Dit is de reden dat op firewalls ingesteld kan worden om niet te reageren op binnenkomende commando's van het ICMP protocol, zoals o.a. gebruikt bij het "ping" commando. Dan is het voor de andere kant net alsof er niemand is. Komt er wel een antwoord, dan is het duidelijk dat er wel iets is aangesloten en wordt een gerichtere zoekprocedure gestart op aanwezigheid van mogelijke beveiligingslekken.

Firewall

Ping

Zoektochten op internet kunnen uiteraard ook zeer gericht plaatsvinden. Een voorbeeld hiervan is de zoekmachine "Shodan" (www.shodanhq.com). Net zoals Google zoekt naar documenten, video's en foto's, zoekt Shodan naar apparatuur op internet. De resultaten zijn voor iedereen op te vragen.

◀ Via zoekmachine Shodan kan apparatuur op internet gevonden worden.

Maar niet alleen via internet worden bedrijven 'gevonden'. Ook draadloze netwerken zijn een toegangspoort tot bedrijven. Het vervelende aan draadloze netwerken is dat het radiosignaal niet stopt bij het hek, maar ook op de openbare weg nog te ontvangen is. Daarvan wordt dus ook gebruik gemaakt voor een activiteit genaamd "war driving". Hierbij wordt met een auto (of soms op de fiets) rondgereden. Met een laptop, een gevoelige WiFi-ontvanger met antenneversterker en een GPS-ontvanger worden alle opgevangen draadloze netwerken mét hun coördinaten in een database gezet. Het nut van deze 'sport' lijkt nihil, desondanks zijn grote delen van de wereld op deze wijze op de kaart gezet.

War driving

Tot enkele jaren terug was er een website met een inzoombare kaart waarop tot op straatniveau WiFi-netwerken in de Benelux konden worden opgezocht, inclusief naam van het netwerk, de beveiligingsstatus (wel/geen beveiliging, welke encryptie) en de leverancier van de apparatuur. Deze web-

Figuur 1 ▶
Deel van een kaart met gevonden WiFi-netwerken *(bron: www.wigle.net)*

site is uit de lucht gehaald vanwege het vele misbruik dat er van werd gemaakt. Inmiddels kan op wigle.net toch weer naar onze regio gekeken worden *(zie figuur 1)*.

Het is uiteraard ongewenst om in een wereldwijd te benaderen database te staan met daarin opgenomen dat het WiFi-netwerk onbeveiligd is. Dat lijkt erger dan het is, want een hacker in China kan geen gebruik maken van uw WiFi-netwerk in Nederland; hij moet daartoe toch echt even langskomen. Maar als er interesse is in uw bedrijf, dan is dat eenvoudig te doen. En mocht het WiFi-netwerk wel beveiligd zijn, dan is het toch nog wel interessant te weten wie de leverancier van de apparatuur is: mogelijk staat in de apparatuur nog steeds het fabriekswachtwoord ingesteld. Mocht dat ook niet het geval zijn maar de WiFi maakt nog wel gebruik van de (al een decennium) verouderde "WEP" encryptie, dan is het nog steeds eenvoudig om binnen te komen aangezien WEP-wachtwoorden binnen seconden te kraken zijn.

WEP

Kortom, ook via WiFi is menig bedrijf eenvoudig te vinden. De kans dat er misbruik van wordt gemaakt is niet groot, maar bestaat wel.

PRAKTIJKVOORBEELD

In 2009 wordt op een website aangekondigd dat op een Nederlandse school iemand een bloedbad gaat aanrichten. Via het IP-adres wordt gevonden dat iemand in Breda deze bedreiging op internet heeft geplaatst en een man wordt door een arrestatieteam van zijn bed gelicht. Hij is echter niet de dader; dit blijkt de buurjongen te zijn, die gebruik heeft gemaakt van het onbeveiligde WiFi-netwerk van zijn buurman.

5.4 MISVATTING: IK HANG NIET AAN INTERNET

Vaak wordt gedacht dat als een systeem geheel losgekoppeld is van internet, dat men dan geen last kan hebben van malware. Dat klopt in zoverre dat vanaf internet niemand rechtstreeks bij het systeem kan. Er wordt dan ook wel gezegd dat het systeem een "air gap" heeft - geen enkele kabel van/naar de buitenwereld.

Air gap

Maar zoals reeds eerder besproken kan malware zich ook via andere methodes verspreiden. Eén van de meest bekende is: de USB-stick. Een virus dat op deze manier een bedrijf binnenkomt omzeilt alle toegangscontroles.

Virus

In het geval van Stuxnet wordt aangenomen dat het virus via een USB-stick van een contractor de opwerkingsfabriek is binnengekomen.

PRAKTIJKVOORBEELD

Een ander gevaar betreft mobiele apparaten die tijdelijk op het netwerk kunnen worden aangesloten. Denk hierbij niet alleen aan het eigen personeel, maar ook aan leveranciers die onderhoud uitvoeren, aan hun producten engineers die helpen met troubleshooting en contractors tijdens de inbedrijfname. Is er apparatuur voorzien van een GSM abonnement, dan is er (onbedoeld) toch een internetkoppeling tot stand gekomen.
Ook steeds gebruikelijker zijn remote diagnostiek modules, waarmee een leverancier of via het telefoonnet of via internet op afstand toegang kan krijgen. Hoe nuttig dit ook is, het komt vaak voor dat na afloop van de sessie de toegang niet dichtgezet (beter nog: losgekoppeld) wordt.

Nog een manier om tóch aan internet gekoppeld te zijn: iemand heeft op eigen initiatief een koppeling gemaakt "omdat dit eenvoudig is". Technisch is dit niet moeilijk, maar diegenen die dit zo 'even' regelen zijn vaak niet op de hoogte van de consequenties op cybersecuritygebied. Zeker wan-

neer iemand van thuis een oude WiFi-router meeneemt, op het netwerk aansluit en geen wachtwoord instelt of gebruik maakt van verouderde beveiligingsmechanismen.

5.5 MISVATTING: HET HEEFT GEEN ZIN, ZE KOMEN ER TOCH DOORHEEN

In Hollywood-producties worden hackers vaak als superintelligente nerds neergezet. Dit maakt dat velen een compleet verkeerd beeld van hackers hebben. Er zal een bovengemiddeld IQ aanwezig zijn bij sommigen, maar de meeste hackers maken toch gewoon misbruik van de fouten die gemaakt worden tijdens het gebruik van internet (zowel privé als zakelijk). Enkele voorbeelden:

- Geen wachtwoord, of een voorspelbaar dan wel kort wachtwoord;
- Openen van attachments in e-mails;
- Bezoeken van dubieuze websites;
- Download van onbekende bestanden;
- Goedgelovigheid;
- Onbekendheid met basisbeveiligingseisen.

Alleen al via deze zes punten worden veel 'hacks' mogelijk. De eerste barrière is dan genomen, de malware kan zich op een systeem nestelen en dan verder werken.

Ook bedrijven maken vaak dezelfde fouten; enkele voorbeelden:

- Slecht beveiligde webservers;
- Gebruik maken van software met bekende lekken;
- Softwareontwikkeling zonder aandacht voor cybersecurity;

Backdoor

- Aanbrengen van 'backdoors' zonder dit aan klanten mee te delen;
- Voorspelbare of eenvoudig te raden wachtwoorden.

In een telecommunicatiebedrijf is software jarenlang niet gepatcht. Hackers ontdekken dit en kunnen door bekende beveiligingslekken te misbruiken eenvoudig binnenkomen en het hoofdwachtwoord van het systeem in handen krijgen.

PRAKTIJKVOORBEELD

De afgelopen jaren hebben we kunnen constateren dat juist op deze punten veel industriële apparatuur eenvoudig te 'kraken' was. Hier hoeft een hacker dus geen familie van Einstein voor te zijn, het bedrijf dat zijn zaken niet op orde heeft is dan een eenvoudige prooi.

Uiteraard zijn er ook zeer slimme hackers die op ingenieuze wijze door alle beveiligingen in een systeem kunnen heen breken. Die zullen er altijd zijn, net als bankrovers nieuwe manieren vinden om eenvoudig aan geld te komen. Het is aan de beveiligers om de lat zo hoog te leggen dat het risico acceptabel wordt; nul zal het nooit kunnen worden.

5.6 MISVATTING: IK GEBRUIK GEEN WINDOWS.

Microsoft heeft de reputatie dat zijn producten veel fouten bevatten en ook veel beveiligingslekken. Een bedrijf zoals Apple heeft precies de tegenovergestelde reputatie: "Er zijn geen Mac-virussen". Maar dat is niet de enige software waarmee we werken; denk ook aan:

- Acrobat voor het bekijken van PDF documenten;
- Webbrowsers zoals Google Chrome, Firefox en Safari;
- Flash voor het bekijken van animaties;
- Java en JavaScript als algemene programmeertalen;
- SQL als database programmeertaal;
- Ruby On Rails, Perl en PHP als webserver programmeertalen;
- Apache voor webservers;
- Antivirusprogrammatuur;
- SCADA en HMI pakketten;
- Engineeringtools voor het schrijven van applicatiesoftware;

Java

- iOS en Android als OS voor mobiele telefoons en tablets;

Firewall

- Embedded software in switches, firewalls, routers, NAS'en, printers;
- Etc.

In al deze softwarepakketten zitten beveiligingsfouten, ook al durven sommige leveranciers te beweren van niet. Veel (grote) leveranciers volgen nu een vaste (1,2,3-) maandelijkse cyclus waarin nieuwe versies van hun producten worden verspreid, omdat er recent ontdekte lekken in gedicht zijn. Openheid op dit gebied is echter wel paradoxaal: hoe beter een leverancier zijn klantenbestand informeert, des te slechter kan zijn reputatie worden. Anderzijds geldt dat een leverancier die nooit van zich laat horen, of zelfs glashard ontkent dat er producten zijn met beveiligingsproblemen, een veel betere reputatie krijgt.

THINK

Apple heeft het imago dat MacOS geen beveiligingslekken bevat. Maar in maart 2008 dichtte het bedrijf 67 lekken in één update en in maart 2010 nog eens 92. De update naar iOS6 voor iPad's en iPhone loste 197 beveiligingslekken op.

De Google Chrome browser had respectievelijk 50, 15, 14, 47 en 31 lekken in de releases 30 t/m 34; de Firefox browser had er tot en met 2013 in totaal 433; Oracle 104 lekken in de release van april 2014.

In de industriële markt is het niet anders, zo blijkt uit een onderzoek naar de industriële software gedaan door de Russische beveiligingsexpert Positive Technologies (PT). Het bedrijf aarzelt niet man en paard te noemen bij het rangschikken van bedrijven op gebied van aantallen beveiligingsproblemen, het aantal inmiddels opgeloste lekken en de snelheid van oplossen. Ook hier blijken grote verschillen tussen leveranciers onderling. Het volledige rapport is te vinden door via Google te zoeken naar: 'SCADA_analytics_english.pdf'.

SCADA

5.7 MISVATTING: HACKERS KOMEN ENKEL VAN BUITEN

Het zijn niet altijd externe hackers die het op een bedrijf voorzien hebben: ook het eigen personeel of ex-personeel kan toeslaan. Hierover zijn genoeg voorbeelden bekend. Het gaat hierbij vaak om uit de hand gelopen arbeidsconflicten. De IT-systemen zijn dan vaak veel kwetsbaarder dan bij externe aanvallen, vanwege bekendheid met:

- De architectuur van het systeem;
- Wachtwoorden en procedures;
- Zwakke plekken.

Het is daarom van belang om bij vertrekkend personeel login's te blokkeren, gebruikersaccounts op te ruimen, (externe) netwerktoegang af te sluiten, etc.

De auteur verlaat een werkgever. Echter zijn toegangspas wordt niet ingenomen; die is daarna nog vijf jaar geldig.

THINK

Het eigen personeel kan een netwerk ook stilleggen door een fout. Bij Ethernet is dit erg eenvoudig te doen waardoor bijvoorbeeld de netwerkbelasting tot 100% stijgt. Dit laatste kan ook veroorzaakt worden door (eenvoudig te schrijven) software maar ook een kapotte netwerkkaart kan hiervan de oorzaak zijn. Het is mogelijk een Ethernet netwerk tegen overbelasting te beveiligen, maar daar is wel professionele apparatuur voor nodig.

Babbling Idiot

PRAKTIJKVOORBEELD

Op 11 augustus 2007 gaat een netwerkkaart op een PC defect op de luchthaven van Los Angeles. Het interne (Ethernet) netwerk van de douane functioneert dan niet meer vanwege overbelasting. Twintigduizend passagiers kunnen niet tot het land worden toegelaten. Na 11 uur wordt een noodoplossing bedacht; pas na drie dagen is de kapotte netwerkkaart gevonden.

Fouten kunnen natuurlijk ook per ongeluk gemaakt worden. Dan is er natuurlijk geen sprake van een 'hack', maar het effect kan even desastreus zijn.

PRAKTIJKVOORBEELD

De auteur start 's ochtends bij een multinational per ongeluk een zelfgeschreven DHCP-server op een industriële besturing die ook aan het kantoornetwerk aangesloten is. Geen enkele PC kan daarna nog printen, bij de e-mail, internetten, etc. Pas twee uur later is de oorzaak gevonden: mijn software.

HOOFDSTUK 6

INDUSTRIËLE NETWERKEN BEVEILIGEN

6. INDUSTRIËLE NETWERKEN BEVEILIGEN

In de beginjaren van malware liep de verspreiding voornamelijk via floppies. Maar nu is iedereen aan internet gekoppeld en op de fabrieksvloer vormen Ethernet (bekabeld of draadloos) en industriële netwerken andere manieren voor malware om zich te verspreiden.

6.1 DE VELDBUSSYSTEMEN

Er zijn tientallen verschillende soorten industriële netwerken van de 1e generatie, ook wel veldbussen genoemd, die vanaf ca. 1995 op de markt gekomen zijn. Enkele bekende namen op dit gebied zijn Profibus/DP, Interbus, CAN, Sercos, Foundation Fieldbus, etc. die allen zeer veelvuldig gebruikt worden in zeer verschillende industriële toepassingen. Deze systemen zijn nooit ontwikkeld om cyberveilig te zijn, maar dat er nooit malware voor is ontwikkeld is goed te verklaren.

Om virussen via een netwerk te kunnen verspreiden, zijn een aantal functies op een netwerk en de erop aangesloten apparatuur nodig:

a) Een virus moet kunnen “draaien” op apparaat A.
b) Via het netwerk moet de programmacode naar B doorgestuurd worden.
c) Het virus moet zich op apparaat B kunnen nestelen (installeren).
d) Het virus moet kunnen “draaien” op apparaat B.

Stap a) is meestal geen probleem als apparaat A een PC is. Maar daarna wordt het lastig.

Stap b). Uiteraard is het versturen van programmacode via

een veldbus technisch wel mogelijk (tenslotte is programmacode niet meer dan een stapel bytes), maar in de meeste netwerken is het eenvoudigweg niet geïmplementeerd - er kunnen configuratiegegevens worden opgestuurd en I/O statussen worden uitgewisseld, maar meer functionaliteit is niet geïmplementeerd.

Stap c) is bij de meeste industriële apparatuur ook onmogelijk, omdat het installeren van extra programmatuur bijna altijd onmogelijk is, zeker bij embedded besturingen (zoals ook PLC's zijn). Een ander voorbeeld: remote I/O modules voeren hun netwerkprotocol uit in hardware en er is dus geen mogelijkheid om software te installeren. En áls het al mogelijk is om programmacode over te sturen, dan doet elke leverancier dat op een eigen manier. Dat is voor een malware-auteur allemaal erg lastig.

Stap d) is uiteindelijk de meest fatale voor overdracht van malware: de programmacode kan alleen uitgevoerd worden op een gelijke processor als in apparaat A en in eenzelfde systeemarchitectuur. Daarom kan Windows-software niet zomaar draaien op een Mac of een PLC of een embedded
Virus systeem. Dus kan ook een Windows-virus zichzelf niet laten uitvoeren op een remote I/O module.

Kortom, er zijn genoeg factoren (b, c en d) die ervoor zorgen dat er geen malware is die zich kan overdragen via een veldbussysteem.

Hoe zat het met Stuxnet?

Stuxnet Het Stuxnet virus maakte gebruik van een PLC die via een Profibus/DP netwerk aan een frequentieomvormer was gekoppeld. Het door de hacker aangepaste PLC-programma veranderde de toerentallen van de motoren, door de frequentieomvormer "verkeerd" aan te sturen. Er werd dus geen Stuxnet-code via Profibus/DP naar de frequentieomvormers overgezet; deze deden gewoon wat hun opgedragen werd. Ze konden ook niet weten dat er met hoge toerentallen iets kapot zou gaan - die applicatiekennis heeft een frequentieomvormer niet.

Firewalls?

In tegenstelling tot de Ethernet-markt bestaan voor de veldbussystemen geen firewalls, intrusion detection systemen, virusscanners, etc. Gegeven de hierboven beschreven analyse zal er ook weinig behoefte aan zijn. Verder vinden potentiële leveranciers van firewalls de markt te sterk versplinterd, gegeven de grote verscheidenheid aan protocollen.

Firewall

6.2 ETHERNET

Ethernet is de meest gebruikte technologie voor LAN's, zowel thuis als op kantoor en ook op de fabrieksvloer wordt (industrieel) Ethernet zeer veel gebruikt. Omdat de fabrieksnetwerken steeds vaker gekoppeld worden aan de rest van het bedrijf, moet beter nagedacht worden over de bescherming tegen malware.

Ethernet heeft, als typische 70'er jaren technologie, geen enkele standaard aanwezige beveiliging tegen misbruik. In principe mag iedereen alles. Indien iemand op het netwerk kan komen, bijvoorbeeld eenvoudigweg door een laptop met een kabel in een netwerkpoort te prikken, dan kunnen er netwerkberichten verstuurd én ontvangen worden.

Fysieke toegangsbeperking

Het is daarom verstandig om niet-gebruikte netwerkpoorten te blokkeren. Dit kan (softwarematig) via managed switches of (hardware matig) door niet gebruikte netwerkpoorten fysiek te blokkeren en het (eenvoudig) losnemen van een Ethernetkabel uit de switch te voorkomen. Uiteraard houdt dit een doelgerichte hacker niet lang tegen.

◀ Twee voorbeelden van fysieke bescherming van netwerkpoorten die ongewenste toegang tot het netwerk voorkomen

Daarom is het ook aan te raden om de toegang tot switches en routers fysiek af te sluiten (behuizing, kast, kamer).

VLAN's

Virtual LAN's zijn een oplossing om op één fysiek netwerk meerdere geheel gescheiden subnetwerken aan te leggen. Het ene VLAN kan het netwerkverkeer in een ander VLAN niet 'zien', ook al maken beide VLAN's gebruik van dezelfde infrastructuur. Er is dus ook geen onderlinge beïnvloeding mogelijk. Een bedrijf zou bijvoorbeeld meerdere VLAN's kunnen maken voor de financiële administratie, personeelszaken, R&D, etc. maar ook voor de productie. Alhoewel VLAN's van origine nooit bedoeld zijn als beschermingsmaatregel tegen malware, kunnen ze wel helpen.

VLAN's houden op zich malware niet tegen, maar kunnen voorkomen dat virussen het hele bedrijf nazoeken en zichzelf transporteren naar alle andere PC's en besturingen. Verder voorkomen VLAN's dat vertrouwelijke informatie zich kan verspreiden buiten de VLAN-grenzen.

Firewall

Firewalls

Een "firewall" (letterlijk: brandschot) controleert alle inkomende en uitgaande netwerkberichten op ongewenste inhoud. De firewall wordt daartoe als toegangspoort gebruikt en geplaatst tussen twee netwerken, bijvoorbeeld: internet en het kantoor-LAN. Maar het is toegestaan (en ook sterk aan te raden) om meer firewalls te gebruiken, bijvoorbeeld ook tussen het kantoor-LAN en het fabrieksnetwerk en mogelijk zelfs tussen productielijnen onderling. Op deze manier wordt het totale netwerk gesegmenteerd in separaat beveiligde subnetwerken, de eerste stap naar een zgn. "defense in depth" strategie.

Defense in depth

Firewalls kunnen zowel in software worden uitgevoerd, als in hardware. De eerste variant komen we tegen in (bijvoorbeeld) Windows en thuis-routers. Het nadeel van software is de traagheid, het voordeel is de lage kosten. Firewalls in hardware, zijnde een speciale module met een eigen processor en speciale software, zijn veel sneller en dat heeft uiteraard ook weer een prijskaartje.

Let op dat firewalls zelf soms ook kwetsbaar zijn voor hackers vanwege fouten die in de firewall software kunnen zitten. Verder moeten firewalls met deep-packet inspection onderhouden worden om nieuwe soorten aanvallen te kunnen herkennen.

ALARM

Firewall

Firewalls kunnen ook ingesteld worden om inkomende netwerkberichten van onbekende afzenders te negeren. Dit maakt remote diagnose moeilijk, omdat de leverancier dan niet 'van buitenaf' kan inloggen. Om dit wel toe te staan wordt vaak (tijdelijk) een poort op de firewall opengezet. Het probleem hierbij is dat a) de netwerkbeheerder overgehaald moet worden deze poort te openen en b) dat deze poort na afloop weer dichtgezet moet worden, hetgeen vaak vergeten wordt.

◀ Een industriële firewall, met dubbele voedingsaansluiting

Firewalls zijn geen nieuwe technologie; in de zakelijke IT worden firewalls intensief gebruikt. In de consumentenmarkt gebruikte "routers" voor thuisgebruik zit ook altijd een firewall ingebouwd. Industriële routers onderscheiden zich van beide markten op een aantal aspecten:

- Steviger mechanische constructie;
- Voldoen aan zwaardere elektrische omgevingseisen;
- Hogere trillingsbestendigheid, temperatuurbereik;
- 24V voeding, meestal dubbel uitgevoerd (redundantie);
- Foutrelais, om een melding te kunnen geven aan een besturing, of om apparatuur uit te kunnen schakelen;
- Herkenning van typisch industriële protocollen (bijvoorbeeld Modbus/TCP).

Intrusion Detection Systems

Een "Intrusion Detection System" monitort het netwerkverkeer op hackpogingen, vreemde of ongebruikelijke netwerk-

berichten en afwijkingen van het veiligheidsbeleid. Hierover wordt gerapporteerd aan netwerkbeheerders en management. Omdat het alleen om detectie gaat en niet om preventie, zal een IDS verder niets doen aan het tegenhouden van een aanval. Er bestaan echter ook wel "Intrusion Detection and Prevention Systems" die dit wel kunnen.

IDS

Het verschil tussen een IDS en een firewall is dat een IDS actief is op het interne netwerk en dus ook aanvalspogingen van binnenuit het netwerk zelf kan herkennen.

Een IDS kan geheel passief op een netwerk aanwezig zijn en is daarom ook voor hackers niet te vinden en dus ook niet te beïnvloeden. De zwakte van een IDS is dat het alleen maar voorgeprogrammeerde patronen kan herkennen en nieuwe soorten aanvallen dus niet kan herkennen. Er bestaan ook wel zelflerende IDS'en, die na een inwerkperiode 'weten' wat voor een bepaald systeem normaal netwerkverkeer is of niet. Aangezien op industriële netwerken netwerkverkeer volgens regelmatig herhalende patronen verzonden wordt, kunnen zelflerende IDS'en daar veel sneller inleren dan op een kantoornetwerk.

TIP

Opvallend is dat veel intrusion detection systems "open source" zijn. Een bekend open-source IDS is SNORT® van het Amerikaanse beveiligingsbedrijf SourceFire. Andere voorbeelden zijn: Bro, OSSEC, Prelude en Suricata.

False negative
False positive

De kwaliteit van een IDS wordt o.a. afgemeten aan het aantal "false positives" en "false negatives". Een "false positive" is een vals alarm; teveel hiervan maakt dat netwerkbeheerders het IDS gaan negeren. Een "false negative" is een gemist alarm, dat is natuurlijk wel een probleem want hierdoor kan ook een malware-aanval gemist worden.

VPNs

Een "Virtual Private Network" biedt de mogelijkheid om op

een veilige manier netwerkberichten te sturen tussen twee locaties A en B over een tussenliggend onveilig netwerk. Hiertoe wordt een zgn. “tunnel” opgezet tussen A en B. Wat het onderliggende netwerk is, maakt verder niet uit - dit kan Ethernet zijn, maar ook een inbelverbinding (via een serieel modem), of via ADSL of het GSM-netwerk. Netwerkberichten in de tunnel tussen A en B worden gecodeerd; afluisteren is dus wel mogelijk maar zinloos. Applicatiesoftware kan verder werken alsof de VPN tunnel niet bestaat; dit is ideaal voor remote control en/of remote diagnose van systemen.

Een VPN is dus geen middel om malware tegen te houden, integendeel: als op locatie A malware actief is, dan kan die zich via de tunnel verplaatsen naar locatie B. Een oplossing hiervoor is om een VPN te combineren met een firewall. Wel biedt een VPN beveiliging tegen injectie van netwerkberichten onderweg en/of afluisteren ervan. Een sterke encryptie is uiteraard wel gewenst.

Firewall

Protocollen

Ethernet is niet gekoppeld aan een bepaald netwerkprotocol; integendeel, bijna alles is toegestaan. Er is dus ook een grote variëteit aan netwerkprotocollen. In de praktijk wordt zeer veel gebruik gemaakt van de TCP/IP protocolfamilie. Maar deze hebben hun eigen beveiligingsproblemen waardoor aanvullende maatregelen (bovenop de hiervoor besproken mogelijke maatregelen) meestal wel nodig zijn.

Ook de TCP/IP protocolfamilie is al decennia oud. Veel van de ‘oudste’ protocollen zijn ooit ontwikkeld in een tijdperk waarin er nog geen malware bestond. Zulke protocollen sturen bijvoorbeeld wachtwoorden als leesbare tekst over, accepteren alles van iedereen, werken met beheersrechten op een systeem, etc.

Bij gebruik van een PC moet de nodige aandacht besteed worden aan het uitschakelen van TCP/IP mogelijkheden die graag door malware gebruikt wordt, bijvoorbeeld remote toegang tot de harde schijf. Ook firewalls kunnen hierbij behulpzaam zijn.

PRAKTIJKVOORBEELD

Het "Simple Network Management Protocol" (SNMP) is hét protocol voor beheer van netwerkcomponenten op afstand, zowel in de zakelijke IT als in de industriële IT. De actuele versie van SNMP is versie 3, welke op een veilige manier tussen apparaten communiceert. In de praktijk wordt echter nog heel veel de onveilige SNMP versie 1 gebruikt.

OPC

Een in de industrie zeer bekende manier van communicatie tussen apparatuur is OPC (Open Platform Communication, voorheen: OLE for Process Control). Het is een groep van standaarden om leveranciersonafhankelijk te kunnen werken, in eerste instantie vooral gebruikt in SCADA systemen (OPC Data Access), maar inmiddels ook veel breder ingezet.

SCADA

De eerste versies van OPC zijn gebaseerd op Microsoft's DCOM protocol (Distributed Component Object Model), dat communicatie tussen PC's zeer eenvoudig maakt. Uiteraard moeten alle PC's dan wel goed geconfigureerd worden, om niet alles aan iedereen toe te staan. Hier zat nu juist het zwakke punt van heel veel OPC implementaties: deze moesten met beheerdersrechten ingesteld worden, hetgeen zeer ongewenst is. En ook al was dit niet nodig, gebrek aan kennis over de juiste manier van Windows DCOM instellingen maakten dat veel systemen 'even snel' op beheerdersrechten werden ingesteld, "dan werkt het".

OPC is jarenlang berucht geweest vanwege de zwaktes op het gebied van beveiliging. Door de specifieke manier waarop het (onderliggende) DCOM protocol werkte konden firewalls ook weinig bescherming bieden. Inmiddels heeft OPC stappen vooruit gezet op het gebied van beveiliging en zijn firewalls ook inzetbaar. Op internet en bij de OPC gebruikersvereniging (www.opcfoundation.org) is veel informatie te vinden over hoe een systeem met OPC correct geconfigureerd moet worden zodat enkel de minimaal benodigde permissies ingesteld hoeven te worden.

6.3 INDUSTRIEEL ETHERNET

Industrieel Ethernet is een fusie tussen de eerste-generatie industriële netwerken (veldbussen) en standaard Ethernet: de mogelijkheden van beide en dus ook de kwetsbaarheden/onkwetsbaarheden van beide. Industrieel Ethernet is dus net zo kwetsbaar als standaard Ethernet, want de onderliggende technologie is hetzelfde. Wel worden andere protocollen gebruikt (zoals ProfiNet, Modbus/TCP, Ethernet/IP, etc.) en de onbekendheid hiermee in de hackerscene maakt dat ze relatief veilig zijn. Maar dat zal echter niet zo blijven.

Eind 2012 hebben studenten van de universiteit van Augsburg (D) een "ProfiNet Fuzzer" gelanceerd. Het stuurt willekeurige ProfiNet-berichten het netwerk op. Afhankelijk van de kwaliteit van de ProfiNet-implementatie van de ontvanger kan deze het bericht negeren (OK), er op reageren (fout), of crashen (erg fout).

BUG

Daarom is het ook bij industrieel Ethernet van belang om een systeem goed te beveiligen. Hoe dit echter precies moet, hangt af van het gebruikte protocol; er zijn geen standaardregels hierover te geven. Enkele voorbeelden:

a) Voor ProfiNet heeft de gebruikersvereniging in 2013 de 2e versie van de "ProfiNet Security Guideline" uitgegeven (documentnummer 7.002, via www.profibus.com).

b) Voor Ethercat zijn er geen aanbevelingen vanuit de gebruikersvereniging gekomen (www.ethercat.org). Aangezien de opbouw en werking van Ethercat sterk afwijkt van wat gangbaar is in (industrieel) Ethernet, kan malware eigenlijk alleen maar functioneren op de netwerkmaster, tenzij nog met TCP/IP gewerkt wordt.

c) Voor Ethernet/IP heeft de gebruikersvereniging (www.odva.org) drie documenten uitgegeven: "Cybersecurity for industrial control systems" (2012) als inleiding; verder "Securing Ethernet/IP networks" (2011) en "Ether-

net/IP Infrastructure Guidelines" (2007). Begin 2013 is aangekondigd dat het protocol aangepast zal worden ("hardened"). Ook komt er een uitbreiding om het protocol via beveiligde "tunnels" over onveilige netwerken te kunnen voeren.

d) Voor Modbus/TCP zijn er geen aanbevelingen gepubliceerd door de gebruikersvereniging (www.modbus.org). Aangezien het protocol verder geen beveiligingsmogelijkheden heeft, is het zomaar koppelen van Modbus/TCP apparatuur aan een LAN of aan internet zeer sterk af te raden. Vanwege de populariteit van Modbus/TCP, tot voor enkele jaren geleden het meest populaire industrieel Ethernet protocol, is er veel aandacht voor de zwaktes ervan.

ALARM

In 2010 was Modbus/TCP het meest door hackers gezochte protocol op via internet aangesloten apparatuur. Dit is eenvoudig vast te stellen via een "TCP port scan" op poort 502, dit is de standaard toegangspoort voor Modbus/TCP.

Ook Modbus-apparatuur voorzien van seriële (RS-232, RS-485) interfaces kan kwetsbaar zijn, indien deze via een seriële Modbus/TCP converter aangesloten is op het Ethernet netwerk.

6.4 DRAADLOOS ETHERNET

Draadloos Ethernet (ook wel bekend als WiFi) wordt ook toegepast in de industrie en is in veel opzichten even kwetsbaar als bekabeld Ethernet, om de eenvoudige reden dat dezelfde netwerkprotocollen gebruikt worden (bijvoorbeeld TCP/IP).

Maar daarnaast is er de extra kwetsbaarheid: omdat draadloos gewerkt wordt, kan iedereen die in bereik is het netwerksignaal opvangen en uitlezen. En wie een signaal kan opvangen, kan ook netwerkberichten mee gaan sturen.

Anderzijds geldt ook dat wie buiten het bereik van een WiFi-netwerk is, niets kan doen. Dit is een geheel andere situatie dan bij een bekabeld Ethernet: als dit (direct of indirect) aan internet gekoppeld is, kan in theorie de hele wereld er bij. Maar voor een draadloos Ethernet moet een hacker echt in de buurt zijn.

Uiteraard zijn er in WiFi beveiligingsmaatregelen aanwezig, bijvoorbeeld encryptie van data in netwerkberichten. Maar niet alle netwerkberichten kunnen gecodeerd worden (bijvoorbeeld voor netwerkbeheer) zodat aanvallen op afstand op WiFi-netwerken altijd mogelijk blijven.

Encryptie

Om afluisteren nutteloos te maken, kan alle WIFI netwerkverkeer gecodeerd worden. Hiervoor wordt gebruik gemaakt van de encryptiemethodes WEP (Wired Equivalent Privacy) en WPA2 (WiFi Protected Access), aangevuld met diverse varianten hiervan.

WEP
WPA2

WEP is de oudste encryptievariant en is inmiddels opgevolgd door WPA2. De reden hiervoor is dat WEP te 'kraken' is: het gebruik ervan biedt geen enkele bescherming meer omdat gebruikte wachtwoorden binnen enkele seconden terug te rekenen zijn.

ALARM

Ondanks dat er al jaren een veel beter alternatief (WPA2) is, wordt WEP toch nog steeds gebruikt!

WPA2
AES

WPA2 beveiliging is gebaseerd is op het Belgische "Rijndael" algoritme, ook wel bekend als "AES" (Advanced Encryption Standard). Het biedt een zeer sterke encryptie, die ondanks alle pogingen daartoe nog steeds niet gekraakt is.

Uiteraard hangt de sterkte van WPA2 af van het gebruikte wachtwoord. Op internet circuleren genoeg WPA2-kraak-programma's die eenvoudigweg alle bekende wachtwoorden uitproberen (*zie ook hoofdstuk 5*). De keuze van een goed wachtwoord blijft dus ook bij WPA2 van belang!

Jamming

Uiteraard zijn alle draadloze netwerken inherent kwets-baar vanwege hun afhankelijkheid van een (in redelijke mate) ongestoord radiospectrum. Wordt dit met een "jammer" gestoord, dan is er nauwelijks communicatie meer mogelijk. Dat geldt in principe voor elk type draadloos netwerk maar systemen die op basis van frequency hopping werken (zoals Bluetooth) kunnen hier beter mee om gaan.

Denial of Service

Zo'n "Denial of Service" (DoS) aanval moet uiteraard altijd in de directe omgeving van het te saboteren netwerk worden uitgevoerd. Dit sluit aanvallen door willekeurige hackers elders in de wereld uit, maar een op een organisatie of systeem gerichte aanval uiteraard niet.

De WPS-knop

Om het gebruik van WiFi eenvoudig(er) te maken, is de zgn. "WPS" knop (WiFi Protected Setup) bedacht. Hiermee kan een nieuw apparaat eenvoudig aan een bestaand netwerk worden toegevoegd: door het nieuwe apparaat in configu-ratie-modus te zetten en door het indrukken van de WPS-

knop worden beide apparaten aan elkaar gekoppeld zonder verdere poespas met netwerkconfiguratie. Ook is het mogelijk om de koppeling te maken met een 7-cijferige PIN-code.

Door een ontwerpfout zijn er echter geen 10^7 = 10 miljoen unieke pincodes, maar slechts 11000. Een hacker hoeft dus gemiddeld maar 5500 pincodes uit te proberen. Dit is binnen enkele uren te doen.

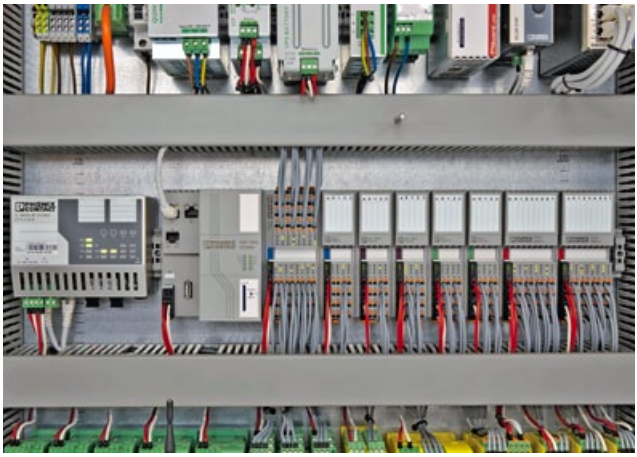
ALARM

Het wordt dus afgeraden om WPS aan te hebben staan op WiFi-netwerken. Bij sommige merken apparatuur is het echter niet mogelijk om WPS uit te zetten.

In industriële WiFi-apparatuur wordt WPS slechts zelden ondersteund, zodat dit probleem zich hier zelden voordoet.

6.5 INDUSTRIËLE NETWERKAPPARATUUR

Op een industrieel netwerk is uiteraard ook de nodige apparatuur aangesloten: PLC's, embedded controllers, displays, remote I/O, intelligente sensoren en actuatoren, motoren, camera's, etc. Kunnen deze ook een rol spelen in de beveiliging?

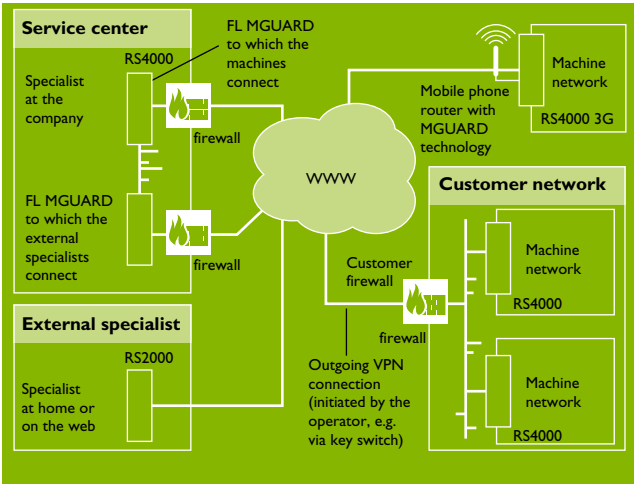


Om deze vraag te beantwoorden moeten we kijken naar hoe een PLC met deze apparatuur, bijvoorbeeld zijn I/O, omgaat. Hoe kan een digitale uitgang 'weten' of zijn status (logische 0 of 1) wordt geregeld door het reguliere PLC programma of een door malware geïnfecteerd PLC programma? Hiervoor zou deze uitgang applicatiekennis moeten hebben, welke dan door iemand geprogrammeerd moet worden en aan de uitgang moeten worden gekoppeld. Maar als malware in staat is om een PLC programma te wijzigen, waarom dan het programma voor de uitgang dan ook niet?

ISA-99
IEC 62443
Firewall

Uiteindelijk bevat een industriële besturing een aantal onderdelen die tegenwoordig via een netwerk aan elkaar gekoppeld zijn, waarbij er een impliciet 'vertrouwen' is tussen deze delen. Een beveiliging wordt daarom alleen geplaatst op de systeemgrenzen. Dit is exact wat beveiligingsstandaarden als ISA-99 / IEC 62443 aanbevelen (*zie hoofdstuk 7*): een 'zone' met 'conduits' (communicatiepaden) die elk beveiligd worden, bijvoorbeeld met firewalls. Daarom wordt aanbevolen om productiecellen en machines afzonderlijk voorzien van een firewall.

Firewalls geplaatst op systeemgrenzen van te beveiligen zones. ▶



HOOFDSTUK 7

STANDAARDEN

7. STANDAARDEN

In de voorgaande hoofdstukken is duidelijk geworden dat de cyberbeveiliging van moderne IT-systemen, zowel thuis, op het werk als op de fabrieksvloer een uitdagende activiteit is. Er is zoveel software, op diverse platformen (PC, embedded, mobiel, ...), gebaseerd op diverse operating systemen (Windows, MacOS, Linux, ...) die soms al bestonden voordat het eerste virus gemaakt werd, werkend met tientallen verschillende netwerkprotocollen (soms 30 jaar oud, soms net nieuw) met allerlei soorten applicaties geschreven in veel programmeertalen door soms jonge onervaren programmeurs, werkend bij bedrijven waar slechts zelden cyberveilig programmeren belangrijk is en gekocht door klanten die helemaal niets weten van IT en cybersecurity en het belang van dit laatste.

Virus

Aan de andere kant van de streep staan soms (jonge) techneuten die de moeite nemen om zeer diep in de materie te duiken om een lek in een programma te kunnen misbruiken. Verder zijn er genoeg hackers die weliswaar niet zoveel weten van IT, maar wel alles van menselijke zwaktes. Op internet is ook zeer veel kant-en-klare software te vinden, zodat een hacker vaak niet echt veel hoeft te weten van de onderliggende technologie en de zwaktes daarin.

Er is dus geen 'silver bullet' die in één klap al onze cybersecurity problemen gaat oplossen en die zal er ook nooit komen. Het zal de komende tijd dus nodig blijven om ons zo goed als mogelijk te beveiligen tegen ongewenst gebruik van onze apparatuur. Niemand hoeft het wiel hier opnieuw uit te vinden: lijsten met tips, aanbevelingen, richtlijnen, standaarden etc. genoeg. En wel zodanig veel dat het ook weer moeilijk is hier een weg in te vinden; veel materiaal is ook niet bruikbaar voor specifiek industrieel gebruik. Het Amerikaanse ministerie van Homeland Security heeft in 2011 een vijftiental normen met elkaar vergeleken en het resultaat in een tabel samengevat; daarmee is eenvoudig te zien dat er een fors verschil in reikwijdte is tussen diverse normen.

WEBSITE

De hiervoor genoemde tabel vind u op www.smartgrid.gov in appendix A "Cross Reference of Standards" van het document "Catalog of Control Systems Security - Recommendations for Standards Developers of Standards".

Uiteraard is het niet mogelijk om in enkele pagina's te herhalen waar anderen honderden pagina's voor nodig hebben. Daarom een korte bespreking van een aantal bekende en veelgebruikte richtlijnen en normen op dit gebied:

- Top-35 van het Australische ministerie van Defensie;
- De SANS Top-20;
- WIB standaard 2784; en
- ISA-99 en IEC 62443.

IEC 62443

7.1 AUSTRALISCHE DOD TOP-35

Het Australische ministerie van Defensie heeft in 2010 de ervaringen bij het beveiligen van de eigen systemen gebundeld in een lijst met 35 punten genaamd "Strategies to mitigate targeted cyber intrusions". Hierin worden de meest belangrijke technieken, procedures en maatregelen opgesomd die genomen moeten worden om systemen veilig te houden. Omdat hackers ook meegaan met de tijd is, gebaseerd op de aanvallen die in 2011 hebben plaatsgevonden, wat geschoven met prioriteiten. Dit document is publiekelijk beschikbaar op www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf

De 35 punten zijn primair ingedeeld naar effectiviteit (essentieel, excellent, goed, gemiddeld). De vier belangrijkste (essentiële) punten zijn:

1) Applicatie whitelisting: alleen toegestane programmatuur mag uitgevoerd worden. *Whitelisting*
2) Patch applicaties: zo snel mogelijk de meest recente patches installeren, om alle bekende lekken te dichten. *Patch*
3) Patch operating systems: idem.
4) Minimaliseren van gebruikers met beheersrechten, zodat geen installatie van software of wijzigingen in systeeminstellingen gedaan kunnen worden.

Volgens de Australiërs zou het implementeren van slechts deze vier punten al 85% van alle cyberaanvallen in 2011 hebben tegengehouden. Het advies is dan ook om met deze vier punten te beginnen, op de meest essentiële systemen en op de PC's van die gebruikers die het meest kwetsbaar zijn. Pas daarna moeten de andere systemen aan de beurt komen, gevolgd door de 31 andere punten uit de lijst. Een aantal punten hebben enkel betrekking op webservers, (minder relevant voor industriële systemen).

Microsoft gaat in de publicatie "Protecting your organisation from targeted cyber intrusion" expliciet in op de 35 Australische punten en hoe die op Windows geïmplementeerd kunnen worden, zonodig met ondersteuning van andere Microsoft producten.

TIP

Opvallend is de overeenkomst met de top-5 uit de lijst van SANS (*zie paragraaf 7.2*); alhoewel in andere bewoordingen gaat het feitelijk om hetzelfde. Opvallend is dat de lijst per punt ook aangeeft wat de verwachte weerstand van de gebruikers tegen de maatregel zal zijn (hoog/midden/laag). Ook geeft de lijst per punt aan wat de initiële investering zal zijn (hoog/midden/laag) en wat de onderhoudskosten zijn (hoog/midden/laag).

7.2 SANS TOP-20

Het SANS (Sysadmin, Audit, Networking, Security) Institute (www.sans.org) is een Amerikaans bedrijf dat zich sinds 1989 bezig houdt met computer security in de breedste zin van het woord, dus ook met industriële cybersecurity. Maar wie zijn industriële installaties 'morgen' al wil beschermen tegen cyberaanvallen, kan niet snel aan de slag - de standaarden van de IEC, ISO, ISA etc. zijn te groot en vragen veel werk.

Daarom heeft SANS zelf een top-20 lijst van te nemen maatregelen vastgesteld. De lijst is gebaseerd op de ervaringen van diverse overheidsinstanties van de VS, Groot-Brittannië en Australië en van bedrijven en personen actief in de cybersecurity. In maart 2013 kwam versie 4.1 van het document uit (www.sans.org/critical-security-controls), om het up-to-date te houden in de zich snel wijzigende wereld van de cybersecurity.

De lijst richt zich op de verdediging tegen de meest gangbare aanvallen, vandaag of in de nabije toekomst, op een geautomatiseerde manier. Eerst komen de "quick wins", eenvoudige maar effectieve maatregelen die het beveiligingsniveau verhogen zonder grote wijzigingen. Daarna wordt de aandacht gelegd op detectie van aanvallen, het tegenhouden / onderbreken er van en verzamelen van informatie. Als derde moet het beveiligingsniveau van de apparatuur omhoog ("hardening") en het aantal zwakke punten worden verminderd. Tenslotte moet de verbetering van de cybersecurity geborgd worden in de organisatie.

De top-20 (van 2013) is als volgt samengesteld:

- Inventory of authorized and unauthorized devices;
- Inventory of authorized and unauthorized software;
- Security configurations for hardware and software on computers;
- Continuous vulnerability assessment and remediation;
- Malware defenses;
- Application software security;
- Wireless device security;

- Data recovery capability;
- Security skills assessment and appropriate training to fill gaps;
- Security configurations for hardware and software on network devices;
- Limitation and control of network ports, protocols and services;
- Controlled use of administrative privileges;
- Boundary defense;
- Maintenance, monitoring and analysis of security audit logs;
- Controlled access based on the 'need to know';
- Account monitoring and control;
- Data loss prevention;
- Incident response capability;
- Secure network engineering;
- Penetration tests and 'red team' exercises.

Red Team

Van elke maatregel wordt in detail verder besproken:

- Welke procedures en (software) gereedschappen er nodig zijn;
- Hoe hackers misbruik maken van de afwezigheid van deze beveiliging;
- Hoe de maatregelen geïmplementeerd moeten worden, beginnende bij de "quick wins" en verder op hogere niveaus;
- Meetpunten en testprocedures voor het vaststellen van de kwaliteit van de implementatie;
- Een lijst van corresponderende maatregelen uit de NIST 800-53 standaard.

De verwijzing naar de NIST 800-53 standaard heeft een duidelijke reden: het is de standaard van de Amerikaanse overheid (voor eigen gebruik), onderdeel van een zeer uitgebreide reeks documenten op het gebied van computerbeveiliging. Wie de SANS Top-20 implementeert, heeft ca. 1/3 van de NIST 800-53 gedaan.

Wie 20 punten nog steeds teveel vindt, kan het beste aan de slag gaan met de "quick wins", die aardig overeenkomen met

de Australische top-4:

Whitelisting

1) Software whitelisting;
2) Beveilig de standaard systemen;

Patch

3) Patch applicaties binnen 48 uur;
4) Patch systeemsoftware binnen 48 uur;
5) Internet browsen of e-mail lezen moet gebeuren zonder admin / root privileges (*zie ook paragraaf 2.3.3*).

SANS zelf schat dat de implementatie hiervan 3 tot 6 maanden duurt.

7.3 DE WIB STANDAARD

Het WIB uit Den Haag (www.wib.nl) is een branche-vereniging van bedrijven die actief in de procesindustrie zijn. Eén van WIB's werkgroepen ("Plant Security") heeft een eigen standaard voor cybersecurity in industriële omgevingen geschreven: "Security Requirements for Vendors".

Aanleiding hiervoor was dat reeds bestaande procedures en standaarden niet echt gericht zijn op de specifieke eisen die in een industriële omgeving gesteld worden en dus niet goed bruikbaar zijn. Ook ligt hier altijd de nadruk op wat de eindgebruiker moet doen, terwijl juist ook de leverancier(s) hard nodig zijn om een goed beveiligd systeem te kunnen maken én onderhouden.

ISA-99
Stuxnet
IEC 62443

De WIB standaard (nummer X-2784) is erg praktisch ingesteld en slechts 50 pagina's groot. Uit onvrede over de langzame voortgang met de ISA-99 standaard (*zie paragraaf 7.4*) is de standaard in 2010 vrijgegeven (vlak na Stuxnet). De werkgroep vond het belangrijk dat bedrijven zo snel mogelijk aan de slag zouden gaan, zodat ook alvast ervaring kon worden opgedaan. Deze zou dan verwerkt worden in een nieuwe versie. Later is besloten om de WIB-standaard te integreren in ISA-99 (inmiddels IEC 62443 *zie hoofdstuk 7.4*).

Opvallend aan de WIB standaard is dat een actieve inbreng van de leveranciers wordt verwacht, die zijn producten op een bepaalde manier dient te ontwikkelen. Ook dienen voor

en tijdens de aanschaf, de installatie en tijdens bedrijf de voorgeschreven procedures gevolgd te worden. De standaard identificeert 35 "Process Areas" (PA), welke in vier categorieën zijn opgedeeld: organizational, system capability, system acceptance testing and commissioning en maintenance & support. De PA's zelf hebben elk een classificatie brons, zilver, goud om een niveau van beveiliging aan te geven (dit dient de leverancier extern te laten verifiëren).

Uiteindelijk schrijft de klant voor wat het minimum beveiligingsniveau van een systeem moet zijn; is dit (bijvoorbeeld) brons dan dienen alle PA's ook minstens niveau brons te hebben. *(zie Figuur 1)*

7.4 DE ISA-99 / IEC 62443 STANDAARD

ISA-99
IEC 62443

De "International Society of Automation" (www.isa.org) is een wereldwijd actieve vereniging met 30000 leden die werkzaam zijn in de industriële automatisering (voornamelijk procesautomatisering). Eén van de activiteiten van de vereniging is het ontwikkelen van standaarden voor nieuwe technologieën bruikbaar binnen de industriële IT. Eén voorbeeld hiervan is de ISA-99 "Security for Industrial Automation and Control Systems", die in 2007 uitgekomen is. Later is het ook een Amerikaanse (ANSI) standaard geworden (ANSI/ISA-99.01.01-2009). Hierbij aanhakend hoort een Technical Report (ANSI/ISA TR99.03.01) "Security Technologies for Manufacturing and Control Systems", waarin een opsomming wordt gegeven van gereedschappen, maatregelen en technologieën die gebruikt kunnen worden om een industriële installatie te beschermen.

Stuxnet

Het werk aan ISA-99 is niet af; ze wordt doorontwikkeld tot de internationale standaard IEC 62443. Hierin is ook de WIB-standaard opgenomen (*zie paragraaf 7.3*). Een belangrijke reden voor de revisie is dat, na Stuxnet, er een analyse gedaan is op de toenmalige ISA-99: zou deze een systeem beschermd hebben tegen Stuxnet? Hieruit kwamen 35 punten voor verbetering.

Figuur 1 ▼
Een deel van de WIB X-2784 standaard.

Base Practice Objective	Requirements	Level
BP 20.04: Password lifetimes and reuse restrictions	BR: During system testing and commissioning the Vendor's system shall demonstrate that users are prompted to change their passwords [user defined] days prior to expiration, with a default of 30 days.	Bronze
BP 20.05: Persistence of special accounts	BR: During system testing and commissioning the Vendor's system shall demonstrate that service, auto-login and operator accounts are configured so that they never expire nor become disabled automatically.	Silver
BP 20.06: Role-based access for network devices	BR: During system testing and commissioning the Vendor's system shall demonstrate that encryption is used during administration of network devices within the ASD over Ethernet.	Silver
	RE (1): During system testing and commissioning the Vendor's system shall demonstrate that network devices have passwords encrypted within the device.	Silver
	RE (2): During system testing and commissioning the Vendor's system shall demonstrate that network devices are implemented with role-based access (e.g. separate passwords for administrators and operators).	Gold

Op het moment van schrijven van deze tekst is de nieuwe versie van de standaard ISA-99 / IEC 62443 nog volop in ontwikkeling. Via de website http://isa99.isa.org kunnen actuele versies van hoofdstukken gelezen worden.

7.4.1 OPBOUW IEC 62443

De standaard is verdeeld in een aantal hoofdstukken:

General

- 1-1 Terminology, concepts and models
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-4 Industrial Automation Control Systems (IACS) security lifecycle and use-case

Policies and procedures

- 2-1 Requirements for an IACS security management system
- 2-2 Implementation guidance for an IACS security management system
- 2-3 Patch management in the IACS environment
- 2-4 Requirements for IACS solution suppliers

System

- 3-1 Security requirements for IACS
- 3-2 Security levels for zones and conduits
- 3-3 System security requirements and security levels

Components

- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS components

Hierbij wordt dus niet alleen gekeken naar hoe een eindgebruiker zijn systemen moet beveiligen, maar óók naar leveranciers, bijvoorbeeld in hoofdstuk 2-4 en 4-1. Hoofdstukken 2-1, 2-2, 2-3, een deel van 2-4 en 4-1 beschrijven processen en procedures; hoofdstukken 2-4, 3-2, 3-3 en 4-2 beschrijven eisenpakketten, de andere hoofdstukken zijn informatief.

De standaard is een “framework”: ze schrijft enkel voor wat er gedaan moet worden om een systeem te beveiligen, maar niet hoe. Dit laatste is ook onmogelijk gegeven de snelle ontwikkeling van de technologie en uiteraard de grote ver-

schillen in systemen die beveiligd moeten worden en hun specifieke wensen. De standaard beschrijft enkel functies in industriële systemen, geen specifieke industrieën, geen types besturingen, geen leverancier(s) en geen specifieke technologieën.

Information Security Management System
Concreet vraagt de IEC 62443 om het inrichten van een "Information Security Management System" (ISMS) voor een "Industrial Automation and Control System" (IACS). De standaard geeft aan hoe dit moet, maar de concrete invulling ervan moet men zelf doen, afhankelijk van de bedrijfsvisie en een uit te voeren risicoanalyse. Ook het inrichten van de organisatie, de implementatie en het borgen van de te volgen procedures moet (uiteraard) zelf gedaan worden.

De standaard vergelijkt zichzelf met een tafel met drie poten; deze blijft enkel staan zolang alle poten aanwezig zijn. De drie poten waar het hier om gaat zijn:

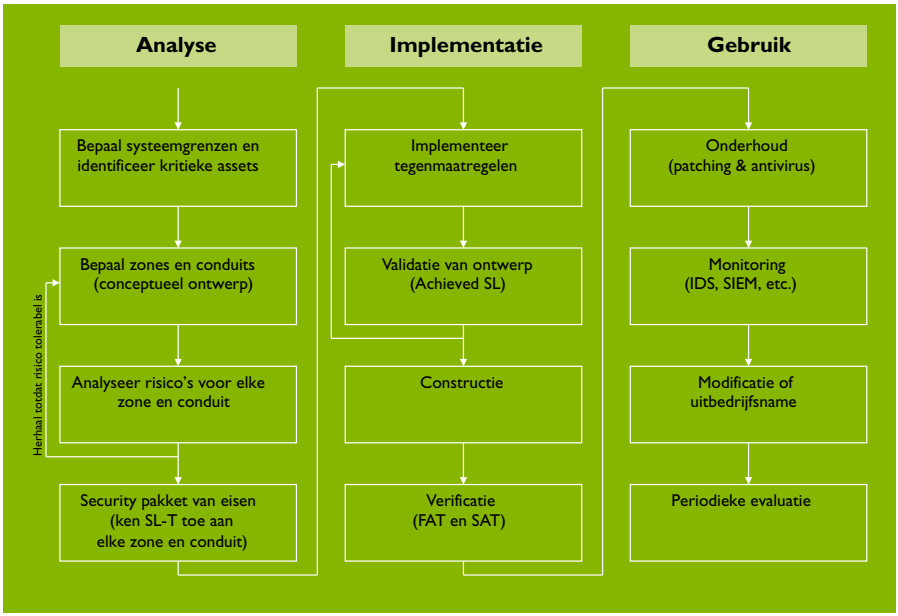
- Mensen;
- Technologie en
- Processen.

De IEC 62443 houdt zich uitdrukkelijk niet bezig met de "mensen". De lezer wordt geadviseerd zich elders te (laten) onderwijzen op het gebied van leiderschap, veranderingsmanagement, bedrijfssociologie, HRM, etc. Op het gebied van technologie definieert de standaard zeven zogenaamde "Foundation Requirements" (*zie hoofdstuk 7.4.4*) en een elftal processen en procedures over:

- Security Policy;
- Organization of Security;
- Asset Management;
- Human Resources Security;
- Physical and Environment Security;
- Communications and Operations Management;
- Access Control;
- System acquisition, development and maintenance;

- Incident Management;
- Business Continuity Management;
- Compliance.

De IEC 62443 geeft ook een stroomschema voor een implementatie (*figuur 2*). In de praktijk zullen deze stappen niet zo strikt na elkaar uitgevoerd worden, maar meer iteratief, zeker de eerste keer.



▲ **Figuur 2**
Stroomschema voor implementatie (volgens IEC 62443).

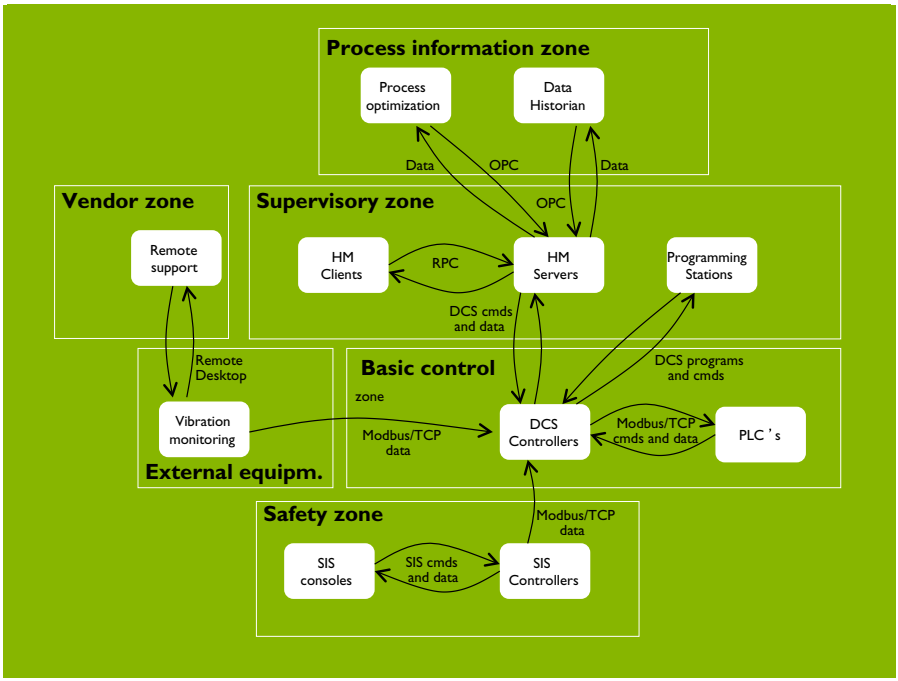
7.4.2 SECURITY MODEL

De standaard onderkent dat het niet mogelijk is om alle componenten met software veilig te maken voor malware. Daarom wordt de nadruk gelegd op de netwerkarchitectuur, waar immers veel meer controle over is, zowel tijdens de aanschaf, installatie als in bedrijf. Een netwerk in een applicatie moet niet bestaan uit één groot netwerk waar iedereen met iedereen kan communiceren en iedereen alles mag en kan; dit is de ideale omgeving voor malware. Een opdeling van een netwerk in "security zones" is daarom de eerste stap. Daarna wordt geanalyseerd welke communicatiepaden

("conduits") er tussen de zones liggen en hoe die zones en conduits dan beveiligd moeten worden.

Zones

De definitie van een 'zone' is een groep logische of fysieke componenten (assets) met gelijke beveiligingseisen. Een zone heeft een duidelijke afbakening (logisch of fysiek) zodat duidelijk is wat wel en wat niet in de zone zit. Eén van de eerste activiteiten volgens de IEC 62443 procedure is dan ook: stel vast welke zones er in het systeem zitten.



Figuur 3 ▲
Voorbeeld van indeling in zones, met de datastromen daartussen (volgens IEC 62443)

Zoals te zien in *figuur 3* kan een leverancier ook een zone zijn. Puur alleen het definiëren hiervan maakt dat al nagedacht moet worden over vragen zoals: hoe zit de beveiliging van die zone in elkaar? En welke risico's loop ik dan als die leverancier gehackt is en toegang tot mijn systemen wil?

Van elke zone wordt een beschrijving en analyse gemaakt:

- Beschrijving van de zone, functie, apparatuur, etc.;
- Logische grens en fysieke grens (indien van toepassing);
- Risicoanalyse:
  - Huidige cybersecurity sterktes / zwaktes;
  - Mogelijke bedreigingen en zwaktes;
  - Consequenties van verlies / stilstand productie;
- Communicatie van / naar andere zones;
- Gebruikte conduits (zie hieronder);
- Te kiezen beveiligingsstrategie (Security Level Target SL-T, zie beneden).

Conduits

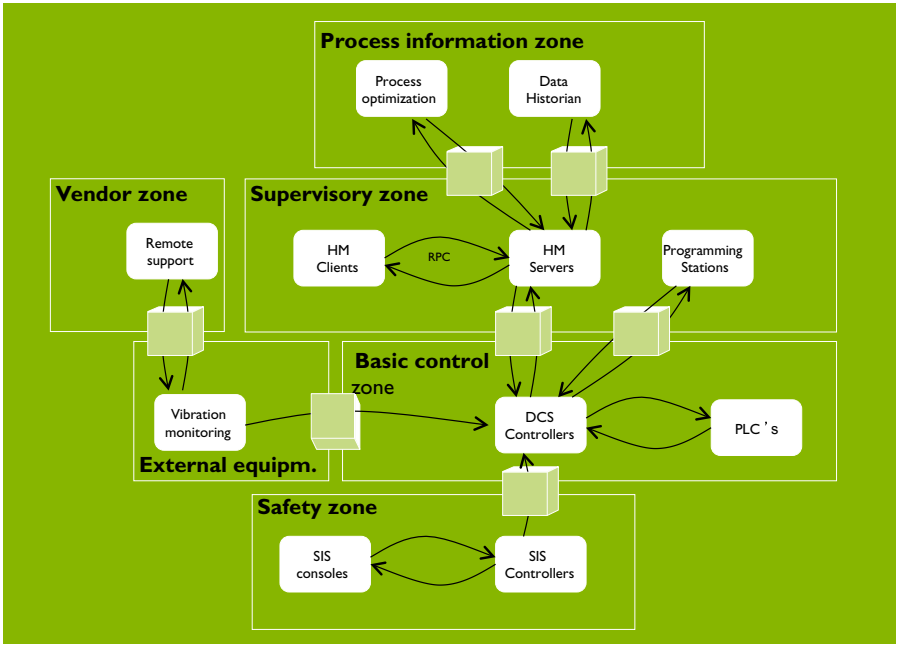
Om te kunnen functioneren, moet er over de zonegrenzen heen gecommuniceerd worden. Hiervoor worden "conduits" gedefinieerd: een conduit is een communicatiepad tussen twee zones en bevat de beveiligingsmaatregelen om deze communicatie veilig te kunnen laten verlopen.

In de standaardtekst wordt het begrip 'conduit' uitgelegd aan de hand van een analogie: een kabelgoot. Deze beschermt de kabels die er in liggen. Een kabelgoot in een gebouw is heel anders dan een kabelgoot buiten een gebouw, waar hogere eisen aan gesteld worden.

Afhankelijk van de aan elkaar gekoppelde zones en de soort communicatie moet de conduit mogelijk een sterkere beveiliging krijgen of kan mogelijk volstaan worden met een eenvoudiger beveiliging. Alhoewel het bepalen van de zones vaak niet al te moeilijk is, is het bepalen van welke datastromen er tussen zones lopen vaak veel lastiger.

Let op dat er ook verborgen conduits kunnen zijn: bijvoorbeeld een werknemer kan data in zone A op een USB-stick schrijven, dan naar zone B lopen en de USB-stick dan weer uitlezen. Zo kan malware dus ook ongezien 'meeliften'. Afhankelijk van de analyse moet deze conduit-te-voet dus ook beveiligd worden; in veel organisaties worden bijvoorbeeld USB-poorten op PC's afgekoppeld.

Een conduit kan ook bestaan tussen een bedrijfsexterne zone (leverancier) en een eigen zone, bijvoorbeeld voor remote-diagnose toepassingen via inbelmodems of internet.



Conduits tussen alle ▲ zone-overgangen.

ALARM

De ervaring bij het uitvoeren van security audits leert dat er vaak veel meer conduits zijn (vaak geheel onbekend) dan in eerste instantie gedacht. Vaak zijn deze ooit aangelegd of geïnstalleerd met een bepaalde reden, maar op een bepaald moment vergeten.

Firewall
Datadiode

Aangezien conduits de in- en uitgangspoorten van alle zones zijn, moet de beveiliging hier geregeld worden, bijvoorbeeld via een firewall, datadiode, VPN tunnel of fysieke maatregelen. Een firewall kan eenvoudig worden

ingesteld om alleen van te voren bekende communicatiepaden toe te staan, bijvoorbeeld van applicatie X op besturing A naar applicatie Y op besturing B. Firewalls met DPI (Deep Packet Inspection) kunnen nog verder gaan, door ook te controleren op de inhoud van netwerkberichten. Datadiodes staan alleen netwerkverkeer in één richting toe. VPN tunnels voeren encryptie uit op netwerkberichten zodat deze over onbeveiligde externe netwerkverbindingen (bv. internet) gestuurd kunnen worden, waardoor afluisteren zinloos is. Fysieke maatregelen kunnen bestaan uit het blokkeren van USB-poorten en Ethernet-poorten op switches / routers, maar ook uit toegangscontroles op gebouwen / ruimtes.

Deep packet inspection

7.4.3 SECURITY LEVELS

Gegeven de zone/conduit analyse, kan een "security level" SL1 t/m 4 vastgesteld worden voor elke zone en conduit. SL1 is het minimum waaraan voldaan moet worden; SL4 is het maximum, waarbij men (in theorie) in staat zou moeten zijn om een Stuxnet-achtig virus te kunnen stoppen. Daar zit natuurlijk wel een prijskaartje aan; voor de gemiddelde systemen zou SL2 haalbaar moeten zijn zonder al te grote investeringen. Een organisatie kan zelf beslissen welk SL het meest zinvol is.

Stuxnet Virus

De standaard maakt vervolgens onderscheid tussen:

SL-T Target Security Level
Gewenste SL voor een bepaald systeem, zoals bepaald uit een risico-analyse.

SL-A Achieved Security Level
Gehaalde SL voor een bepaald systeem, bepaald zodra het in gebruik is.

SL-C Capability Security Level
SL dat gehaald kan worden indien het correct geconfigureerd is.

De SL-T wordt bepaald tijdens de security assessment; de SL-A is wat na implementatie bereikt is. De SL-C wordt door de leverancier opgegeven.

7.4.4 FOUNDATION REQUIREMENTS

Per zone en per conduit wordt nu verder ingezoomd op alle aspecten die van belang zijn voor een goede beveiliging. Dit is de technische kant van de IEC 62443, welke hiertoe zeven "Foundation Requirements" (FR) noemt:

FR1	IAC	Identification & Authentication Control
FR2	UC	Use Control
FR3	SI	System Integrity
FR4	DC	Data Confidentiality
FR5	RDF	Restricted Data Flow
FR6	TRE	Timely Response To Events
FR7	RA	Resource Availability

Per FR is een concrete invulling van wat er moet gebeuren op elk SL (Security Level); als voorbeeld die van FR 6 "Timely Response to events":

Level	Monitor the operation of the control system and respond to incidents when they are discovered by …
SL1	… collecting and providing the forensic evidence when required.
SL2	… actively collecting and periodically reporting forensic evidence.
SL3	… actively collecting and pushing forensic evidence to the proper authority.
SL4	… actively collecting and pushing forensic evidence to the proper authority in near real-time.

Hoe dit gedaan moet worden, is per FR nog verder uitgewerkt in individuele "System Requirements" (SR). Het aantal is per FR verschillend; voor FR6 zijn bijvoorbeeld 2 SR's beschreven. Verder kunnen er nog additionele eisen

("Requirement Extensions", RE) gesteld worden voor de hogere SL's. Een voorbeeld:

SR6.1	Audit log accessibility: the control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.
SR6.2	Continuous monitoring: The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.
RE1	The control system shall provide programmatic access to audit records using an application programming interface (API).

Indien volstaan kan worden met SL1 (Security Level 1), hoeft enkel SR6.1 geïmplementeerd te worden. Voor SL's 2, 3 en 4 moet ook SR6.2 geïmplementeerd worden. Voor SL's 3 en 4 moet additioneel nog RE1 gevoegd worden.

In de standaard is elke SR uitgewerkt, waarin genoemd is wat er gedaan moet worden, maar niet hoe (soms worden er wel wat voorbeelden gegeven).

Implementatie

Na de analysefase kunnen de gekozen beveiligingsmaatregelen, processen en procedures geïmplementeerd worden. Mogelijk blijkt dan dat niet alles gedaan kan worden zoals oorspronkelijk gedacht, bijvoorbeeld vanwege technische of financiële redenen, of omdat nieuwe soorten bedreigingen de kop opsteken. Dan moet de bestaande analyse deels opnieuw gedaan worden; de werkwijze in de praktijk is niet altijd zo lineair als de standaard suggereert.

Uiteindelijk is de implementatie klaar. Het systeem heeft nu een “Security Level Achieved” (SL-A). Deze moet minstens gelijk zijn aan de eerder bepaalde SL-T (Security Level Target). Zo niet, dan is nogmaals een iteratie nodig.

In bedrijf

Cybersecurity houdt niet op als een systeem eenmaal in bedrijf genomen is. Dagelijkse aandacht is nodig voor meldingen in de logbestanden. Veel aandacht is er in de IEC 62443 ook voor patchmanagement van alle systeemcomponenten met software (*zie ook hoofdstuk 8*).

Systemen veranderen; besturingen kunnen toegevoegd / verplaatst worden, software wordt aangepast, nieuwe deelnemers worden op het netwerk toegevoegd, nieuwe leveranciers worden actief, productieprocedures kunnen wijzigen, nieuw personeel stroomt in, etc. Dit kan allemaal gevolgen hebben voor de beveiliging. Ook al is het systeem op dag #1 optimaal beveiligd (voor zover mogelijk), actief onderhoud aan het beveiligingsbouwwerk blijft nodig. Indien dit verslapt, is na enige tijd de beveiliging een gatenkaas en zonder dat dit opvalt.

Incidenten

Cybersecurity-experts gaan er van uit dat elk systeem een keer aangevallen wordt, al dan niet doelbewust. De vraag is dan, hoe gaan we daarmee om. Net zoals de brand- en ontruimingsoefeningen in een bedrijf gedaan worden, moeten cybersecurity-incidenten geoefend worden: wie heeft de leiding, wie doet wat wanneer, welke procedures worden gevolgd, etc. Laat geen kostbare tijd verloren gaan waardoor nog meer schade aangericht kan worden. Oefen ook het terugrollen van backups, herinstallatie van software, herconfiguratie van systemen, etc. Denk hierbij ook aan het feit dat bestanden die van websites van toeleveranciers gehaald moeten worden, mogelijk niet meer beschikbaar zijn na een aantal jaar. Ook is er misschien geen internetverbinding beschikbaar of actief.

7.5 MEER INFORMATIE

De hierboven beschreven procedures en standaarden zijn maar een klein deel van beschikbare standaarden en procedures op het gebied van industriële cybersecurity. Leveranciers hebben vaak nog eigen documentatie op dit gebied, evenals brancheverenigingen. Wie met Windows werkt, kan op dit gebied ook nog wel het nodige vinden.

Een kort overzicht van andere standaarden, procedures en documenten:

AGA 12	Cryptographic protection of SCADA communications
API 1164	Pipeline SCADA security
6 CFR Part 27	Chemical Facility Anti-Terrorism Standard
CIDX	Chemical Industry Data Exchange
FIPS 199	Standards for Security Categorization for Federal Information Systems
FIPS 200	Minimum Security Standards for Federal Information Systems
IEEE 1686	Substation IED Cyber Security
IEEE 1689	Serial SCADA Links and IED Remote Access
ISO 27001..12	Information Security Standards
ISO 27032	Guidelines for cybersecurity
ISO 15408-3	Evaluation Criteria for IT Security
NERC CIP 002	Critical Cyber Asset Identification
NERC CIP-003	Security Management Controls
NERC CIP-004	Personnel and Training
NERC CIP-005	Electronic Security Perimeter(s)
NERC CIP-006	Physical Security of Critical Cyber Assets
NERC CIP-007	Systems Security Management
NERC CIP-008	Incident Reporting and Response Planning
NERC CIP-009	Recovery Plans for Critical Cyber Assets
NIST SP800-82	Guide to Industrial Control Systems Security
OLF 104	Oil Industry Association

NERC

HOOFDSTUK 8

AAN DE SLAG

8. AAN DE SLAG

In de voorgaande hoofdstukken is te lezen dat cybersecurity geen “silver bullet” heeft die in één klap en voor altijd alle hackers en malware buiten de deur houdt. In hoofdstuk 7 zijn een aantal beveiligingsstandaarden besproken, waaruit blijkt dat het opzetten van een goede beveiliging veel werk is. In dit hoofdstuk zullen we enkele van de belangrijkste aspecten van een beveiligingstrategie bespreken.

8.1 KEN DE KARAKTERISTIEKEN VAN MALWARE

Wie geen IT-achtergrond heeft, kan soms moeilijk begrijpen waarom zoveel verschillende beveiligingsmaatregelen nodig zijn. Als we kijken naar een analogie: hoe medici te werk gaan met échte virussen en bacteriën, zal dit duidelijker worden.

Virus

Een ‘gewoon’ virus verspreidt zich over mensen en maakt ons ziek. Eén van de manieren waarop een ziekte bestreden wordt, is het voorkomen van de verspreiding, bijvoorbeeld door isolatie. Is verspreiding niet te stoppen dan kan infectie soms voorkomen worden door (voortijdige) inenting. En als besmetting toch heeft plaatsgevonden, is een medische behandeling nodig, waarbij of het virus wordt bestreden, of de gevolgen ervan, of beide.

Malware
Air gap

Met software-virussen (en andere malware) zien we eigenlijk hetzelfde. Het wil zich verspreiden naar andere systemen en die dan infecteren. Kunnen we deze verspreiding voorkomen, dan is al veel gewonnen. Complete isolatie van systemen is soms een oplossing, de zogenaamde “air gap”: er is dan geen enkele netwerkverbinding met de rest van de wereld. Soms gaat dat echter niet en daarom is een antivirusscanner nodig of andere technieken om malware tegen te houden. Helpt ook dit niet, dan

moet een systeem opgeschoond worden of opnieuw geïnstalleerd.
Samenvattend kunnen we de volgende stappen nemen in de bestrijding van malware:

a) Voorkomen van verspreiding;
b) Voorkomen van installatie;
c) Voorkomen van activering;
d) Detectie;
e) Opruimen en opschonen.

8.1.1 VOORKOMEN VAN VERSPREIDING

De meeste malware wil zichzelf graag verspreiden naar andere systemen. Dat houdt dus in dat de programmacode overgedragen moet worden. Dit kan met alle media waarop programmacode verplaatst kan worden:

- Een netwerk (bekabeld of draadloos, LAN of internet);
- Via een website (veel webpagina's voeren programmacode uit in de browser);
- Een bijlage (attachment) in een e-mail;
- Een USB-stick of iets gelijksoortigs (bijvoorbeeld losse harde schijf);
- Een mobiele telefoon;
- Floppies en tapes.

Het blokkeren van de verspreiding van malware moet dus op diverse fronten gebeuren; het heeft geen zin om gebruik van USB te verbieden maar tegelijkertijd wel onbewaakt internetgebruik toe te staan.

Uiteraard zijn hackers ook op de hoogte van deze beschermingsmaatregelen en pogen dan toch door de controles van het systeem heen te breken. Bijvoorbeeld: een e-mailprogramma kan waarschuwen dat een attachment aan een e-mail geen tekstbestand is, maar een programma. Dan komt de melding "Onbekende bron; toch executeren (j/n)?" De lezer vertrouwt het niet, maar ziet dat de e-mail van een collega afkomt, dat zal dus wel in orde zijn en klikt op "ja" en wordt alsnog geïnfecteerd.

Hoe krijgt een malware-auteur dit voor elkaar? De sociale media spelen hierbij een steeds belangrijker rol, aangezien hier heel veel nuttige persoonlijke en professionele informatie op te vinden is.

PRAKTIJKVOORBEELD

Stel een hacker wil bij één specifiek bedrijf binnenbreken. Er wordt op LinkedIn gezocht naar een werknemer van dat bedrijf. Dan is Facebook aan de beurt: welke hobby's heeft hij? Hiermee wordt de tekst van de e-mail in elkaar gezet. Dan is LinkedIn weer aan de beurt, op zoek naar een collega, in wiens naam de e-mail verstuurd gaat worden. Dan wordt die e-mail via een gehackte PC elders in de wereld verstuurd (zodat de hacker niet na te speuren is). Aan de e-mail wordt een attachment mét malware gehecht waarop geklikt moet worden; de tekst in de e-mail moet de lezer hiertoe verleiden. Inmiddels heeft het aanstaande slachtoffer de e-mail binnen, leest de tekst van de collega over zijn hobby, klikt in vol vertrouwen ("Wie kan dit nu allemaal weten?") op de bijlage, waarna de infectie een feit is.

Blokkades

Omdat de genoemde overdrachtsmethodes sterk van elkaar verschillen, zijn ook diverse maatregelen nodig om malware te blokkeren:

- Bewustwording bij het personeel: hoe om te gaan met e-mails met attachments, websites, gevonden of als cadeau ontvangen USB-sticks.
- Uitschakelen van de USB-poorten op een PC. Door ze fysiek te verwijderen (indien mogelijk), dicht te lijmen, of anderszins te blokkeren.
- Blokkeren van internet-toegang op industriële systemen.

Een blokkade van USB zal veel commentaar opleveren omdat USB tegenwoordig vaak de enige methode is om data tussen (standalone) systemen over te dragen. Hier zal een werkbare oplossing voor gevonden moeten worden, anders zal de blokkade genegeerd of omzeild worden door het eigen personeel.

PRAKTIJKVOORBEELD

IT-bedrijf IBM deelde USB-sticks uit aan de bezoekers van de Australische AusCERT 2010 beveiligingsconferentie. Later bleek dat deze USB-sticks besmet waren met malware.

8.1.2 VOORKOMEN VAN INSTALLATIE

Malware wil zichzelf graag op een systeem installeren, zodat het bij elke opstart weer (opnieuw) actief kan worden. Als we installatie dus kunnen voorkomen, is de malware tegengehouden. Denk hierbij aan:

- "Read only" maken van media / geheugendragers / netwerk (voor zover mogelijk);
- Geen gebruik maken van administrator / root accounts;
- Gewone gebruikers geen installatierechten geven;
- Elke gebruiker alleen die rechten geven die nodig zijn voor uitvoering van zijn werkzaamheden (principe van "least privilege");
- Controles op opstartconfiguratie van een systeem (veel virusscanners doen dit);
- Controles op (ongewenste) wijzigingen in bestanden;
- "Gast" accounts blokkeren;
- Alle accounts voorzien van een (sterk) wachtwoord;
- Etc.

Stuxnet

Let erop dat het niet alleen om PC's gaat; een deel van Stuxnet installeerde zich ook op een PLC (*zie hoofdstuk 4*) door modificatie van het PLC-programma in de engineering database.

Ook al zijn alle technische maatregelen genomen om installatie te voorkomen, dan kan malware zich soms tóch nog installeren. Dit is mogelijk omdat misbruik wordt gemaakt van beveiligingslekken in software. Door ervoor te zorgen dat geen bekende beveiligingslekken op een systeem aanwezig zijn, kan malware zich op deze manier dus ook niet (meer) installeren. Alleen beveiligingslekken waar nog geen

oplossing voor is maken een systeem dan kwetsbaar. Hier kunnen de andere beveiligingsstappen helpen.

Het verwijderen van (bekende) beveiligingslekken op een systeem geschiedt door het overschrijven van de onveilige software door een betere versie. Dit heet "patchen" en wordt in hoofdstuk 8.2 beschreven.

Patch

8.1.3 VOORKOMEN VAN ACTIVATIE VAN MALWARE

Omdat alle malware een computerprogramma is, kan het actief worden als het mogelijk is om een programma uit te voeren. Dat is uiteraard geen vreemde vraag voor een computer of besturing en daar maakt malware graag gebruik van. Het blokkeren van opstartmogelijkheden voor ongewenste programma's is dus een effectieve blokkade van malware.

Helaas zijn er zeer veel mogelijkheden om programma's op te starten. Nemen we als voorbeeld Windows. Dit heeft de volgende mogelijkheden:

- Drivers (voor hardware);
- Systeemdiensten (voor ondersteuning van de gebruiker);
- Gebruikersapplicaties;
- Macro's (zoals in Word en Excel);
- Interactieve applicaties via een webbrowser: JavaScript, Java, Flash;
- "autorun" programmatuur op USB-sticks, CD-ROM's, DVD's;
- SQL scripts (voor database manipulatie);
- Webserver scripts.

Java

Het is dan ook niet verwonderlijk dat malware-auteurs al deze mogelijkheden gebruiken. Een bescherming hiertegen is dus geen kwestie van ergens één vinkje aanzetten; op alle hierboven genoemde gebieden zal iets gedaan moeten worden! Bijvoorbeeld:

- Drivers moeten een digitale handtekening hebben; zo niet dan wordt de gebruiker gevraagd of installatie mag;
- Macro's kunnen in Word en Excel standaard uitgezet

worden;

- Java en Flash moeten van het systeem verwijderd worden;
- "autorun" wordt op Windows niet meer automatisch gedaan (tenzij het toch weer geactiveerd is).

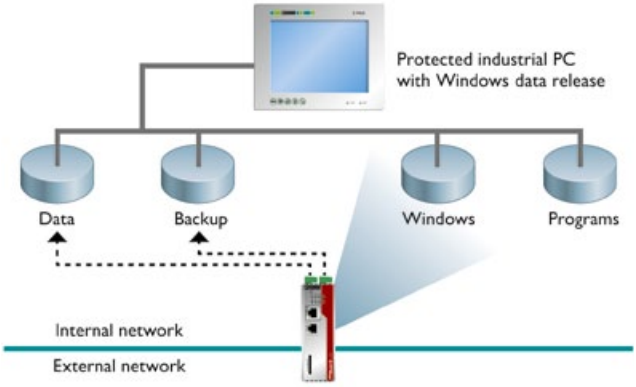
Whitelisting

Het is ook in Windows mogelijk om met "whitelisting" te werken, bijvoorbeeld Microsoft's AppLocker in Windows7 of SoftwareRestrictionPolicies in XP en Vista of een product van een andere leverancier. Dan kunnen alleen die applicaties gestart worden waarvoor dit toegestaan is. Op een normale PC is dit erg lastig, aangezien gebruikers regelmatig nieuwe programmatuur toevoegen. Maar op een PC in een industriële omgeving is dit veel eenvoudiger: de software is stabiel en er hoeft geen nieuwe software bij te komen. Een heel andere situatie dus dan op veel zakelijke en consumenten-PC's, waar nieuwe software regelmatig wordt geïnstalleerd.

8.1.4 DETECTIE VAN MALWARE

Virus

Aangezien een virus niets anders is dan een computerprogramma (met vaak kwade bedoelingen), moet het ergens in het geheugen geladen worden en regelmatig CPU-tijd toegewezen krijgen. Dit wijkt wat dat betreft niet af van gewone programmatuur, behalve dan dat malware zich via het netwerk zal proberen verder te verspreiden. Detectie van



CIFS Integrity Monitoring op een mGuard firewall detecteert automatisch malware en andere ongebruikelijke programmatuur op een PC. ▶

ongebruikelijke programmatuur op een systeem kan worden geautomatiseerd. Nieuwe bestanden, aangepaste bestanden, gewijzigde configuratie, etc. op PC's kunnen worden herkend door sommige firewalls of virusscanners.

Firewall

Gezien de grote hoeveelheden nieuwe malware, kan een virusscanner alleen maar 'bijblijven' qua kennis door van de leverancier regelmatig (soms meerdere malen per dag!) nieuwe virusdefinities te ontvangen. Hiervoor is dus een actieve internetverbinding nodig en een (betaald) abonnement bij de leverancier. Een virusscanner die niet up-to-date is, heeft eigenlijk geen zin!

Virusscanner

Detectie van vreemd netwerkverkeer is alleen mogelijk als bekend is wat "normaal" netwerkverkeer is: wie communiceert met wie, wanneer, hoe, waarover, hoeveel?

8.1.5 OPRUIMEN VAN MALWARE

Opruimen van malware gebeurt in het algemeen vrij simpel door het wissen van de malware bestanden, terugzetten van de originele bestanden en het opschonen van het register (Windows). Soms is dit echter niet mogelijk omdat de malware uit meerdere delen bestaat die elkaar bewaken; wordt het ene deel gewist dan ziet een ander deel dit en herinstalleert dat dan weer. De enige manier om van dit soort malware bevrijd te raken is het geheel opnieuw installeren van het getroffen systeem. Dat houdt meestal in: formatteren van de harde schijf, gevolgd door herinstallatie van alle software.

Malware

Dit kan een tijdrovende bezigheid zijn, zeker als het onvoorbereid moet gebeuren. Wie honderden megabytes aan software moet laden vanaf diverse websites van leveranciers, die vaak oudere softwareversies niet eens meer online hebben, kan hier héél veel tijd aan besteden (en met de aanname dat internettoegang beschikbaar is).

PRAKTIJKVOORBEELD

Een onbekende hacker heeft de website van het Vlaamse Hulpdiensten Forum (HDFV) gewist, waarop de afgelopen 10 jaar foto's en berichten over branden en (verkeers)ongevallen geplaatst werden door honderden vrijwilligers. Ook de backup is gewist.

Een goede backup is eigenlijk essentieel, niet enkel vanwege cybersecurity, maar ook vanwege andere calamiteiten (kapotte apparatuur, brand, waterschade, etc.). Vergeet ook niet om de backupprocedure te oefenen, het zal niet de eerste keer zijn dat zal blijken dat de backup data onleesbaar is.

Patch

8.2 PATCHEN

Het goed "gepatcht" houden van software is een van de belangrijkste activiteiten tijdens de levensduur van een systeem om het beveiligingstechnisch bij de tijd te houden. Daarom staat het ook hoog op de prioriteitenlijst van de in hoofdstuk 7 besproken standaarden. Desondanks is het een activiteit waar systeembeheerders in het algemeen niet warm voor lopen. Ook in de productie wordt patchen vaak op de lange baan geschoven, omdat het bijna altijd productiestilstand oplevert. Diverse bedrijven en (overheids)instanties die de afgelopen jaren het slachtoffer zijn geworden van hackers hadden dit allemaal te danken aan het niet up-to-date hebben van hun systemen.

TIP

Als het specifiek om een beveiligingsprobleem gaat, worden ook vaak de woorden "hotfix" of "security update" gebruikt. Er is echter geen industriebrede consensus over het gebruik van deze woorden, zo lanceert Microsoft wel eens hotfixes om functionele fouten in Windows op te lossen die niet kunnen wachten tot de volgende versie of service-pack van Windows.

Patches bestaan in twee varianten:

1) Om functionele fouten ("bugs") in software te repare-

ren; hierbij gaat het om bestaande functionaliteit die niet werkte zoals eerder beloofd.
2) Om beveilingslekken in software te dichten.

Voor de beveiliging zijn enkel de patches van de 2e variant van belang; de eerste categorie dicht geen beveiligingslekken (installatie is alleen nodig indien men last heeft van de functionele fout).

Het is gebruikelijk dat als een nieuwe release van software geleverd wordt, ook alle bekende functionele fouten opgelost zijn en beveiligingslekken gedicht zijn. Echter, voor nieuwe releases moet in het algemeen betaald worden, terwijl patches bijna altijd kosteloos ter beschikking worden gesteld.

8.2.1 WANNEER IS ER EEN PATCH?

Patch

Zodra een leverancier bekend is met een beveiligingslek in zijn software, kan er een patch voor gemaakt worden. Hoe snel dit gaat hangt geheel af van de prioriteit die er aan gegeven wordt.

Het maken van patches gaat soms erg traag. De leverancier moet hiervoor resources (mankracht, budget, apparatuur) ter beschikking stellen en de mate waarin dit geschiedt bepaalt het tempo waarin de patch vrijkomt. Daarbij zijn veel patches niet eenvoudig: het beveiligingslek moet gedicht worden, maar er mogen geen nieuwe (beveiligings- of functionele-) problemen ontstaan. Uitgebreid testen is dus nodig, ook dit kost tijd.

Het is niet ongebruikelijk dat het uitkomen van een patch soms maanden kan duren, bij sommige leveranciers zelfs jaren. En soms reageert een leverancier helemaal niet op gemelde beveiligingsproblemen, of ontkent ze glashard. Anderzijds zijn er ook leveranciers die patches binnen enkele dagen kunnen leveren.

TIP

Beveiligingsstandaarden als IEC-62443 eisen dat patches binnen een maand na vrijgave door de leverancier worden ingevoerd. Dit is een vrij korte tijd, die in veel organisaties niet gehaald wordt.

8.2.2 HOE INSTALLEERT EEN PATCH?

Een patch is gewoon een stuk software en wordt dus ook geïnstalleerd zoals elke andere software. Bijvoorbeeld op een PC zal het installatiedeel van de patch 'oude' bestanden overschrijven met nieuwe versies hiervan. Bij embedded systemen wordt vaak het gehele geheugen eerst gewist en daarna opnieuw geladen met de nieuwe software. In beide gevallen kan de installatie van een patch erg kritisch zijn, zodat deze niet onderbroken mag worden, bijvoorbeeld door een reset, reboot of power-cycle.

Patch

Hoe wordt de patch actief?

Nadat een patch geïnstalleerd is, is deze nog niet automatisch actief. Er kan immers nog steeds software actief zijn die de "oude" versie nog in het geheugen heeft staan. De patch wordt dus pas effectief als de software opnieuw opgestart is. Op een Windows PC houdt dit in: opnieuw opstarten, of op zijn minst: bestaande programma's afsluiten. Bij embedded systemen houdt het in: geheel opnieuw opstarten. Afhankelijk van de complexiteit van een systeem kan zo'n herstart soms maar enkele seconden kosten, maar ook wel tientallen minuten in beslag nemen.

Waar zit het venijn?

Het feit dat een deel van een systeem tijdelijk niet kan functioneren tijdens installatie van een patch en/of nog eens herstart moet worden, is een probleem voor industriële omgevingen. In een kantooromgeving kan dit eenvoudig aan het eind van de dag of in het weekend gebeuren. Iedereen krijgt een e-mail van systeembeheer "de database is even uit de lucht" en men neemt een korte pauze. Maar het is niet altijd mogelijk elk industrieel systeem te stoppen, ook al is het

maar voor vijf of tien minuten, Dit is één van de belangrijkste redenen dat patchen van industriële systemen zo slecht gedaan wordt.

Uiteraard wordt elk systeem wel eens een keer gestopt, maar dat kan dus best zijn: eens per maand, eens per jaar, tijdens een grootschalige revisie om de vijf jaar, etc. Een patch kan dan dus pas geïnstalleerd worden tijdens zo'n productiestop. Dat houdt dus ook in dat alle bekende beveiligingsproblemen tot die tijd aanwezig zijn en dus ook misbruikt kunnen worden. Dit is de reden dat industriële systemen vaak erg achterlopen op de meest actuele versie van software.

Patch

8.2.3 WORDT ER WEL GEPATCHT?

Dat één keer per jaar de software gepatcht wordt is jammer, maar nog niet zo erg als helemáál niet patchen. De software blijft dan staan op de stand die ze had bij oplevering van het systeem en wordt nooit meer bijgewerkt. Hiervoor zijn twee redenen aan te dragen:

a) Bewust niet patchen: er is een kans, weliswaar klein, dat door installatie van een patch de productiesoftware het niet meer doet. Dat is in een productieomgeving niet acceptabel. Patches worden dan ook alleen geïnstalleerd als de leverancier van de productiesoftware de nodige testen heeft uitgevoerd.

b) Onbewust niet patchen: niemand houdt bij voor welke software in het systeem patches van de desbetreffende leveranciers beschikbaar zijn. Er is dus ook geen (regelmatig) contact met de leverancier(s). Deze weten vaak ook niet welke softwareversies bij welke klanten uitstaan. Daarnaast is het nogal ongebruikelijk om klanten proactief te informeren over het beschikbaar komen van patches; deze worden geacht zelf regelmatig websites na te zoeken.

Het kan ook voorkomen dat software niet gepatcht wordt voor bekende beveiligingsproblemen omdat er geen onder-

houd meer op die software wordt gepleegd omdat de leverancier hier niet meer in wil investeren. Het levert immers geen extra omzet meer op. Liever heeft men dat de klanten overschakelen naar de (te kopen) nieuwste release. Hoe lang 'oude' software nog onderhouden wordt, is geheel leveranciersafhankelijk. Aangezien 'oude' software functioneel veelal prima in orde is, wordt deze eigenlijk nooit vervangen vanwege beveiligingsredenen.

8.2.4 TO PATCH OR NOT TO PATCH

Patches zouden niet nodig zijn als software zonder beveiligingsproblemen (en functionele bugs) opgeleverd zou kunnen worden. Helaas is dit onmogelijk met de huidige stand der techniek. Het zou al een verbetering zijn als patches "hot" geïnstalleerd zouden kunnen worden, zonder enige interruptie in het functioneren van het te patchen systeem. Dat is echter bijna altijd onmogelijk. We zitten dus nog (lang) vast aan het moeten installeren van patches.

Patch

Firewall

Als dit niet snel kan, dan rijst de vraag: is het mogelijk om misbruik van een beveiligingslek te voorkomen tot het moment van installatie van de patch? Het antwoord hierop is: soms wel. Als er een beveiligingslek in een netwerkprotocol zit, worden door de hacker speciale netwerkberichten gegenereerd om van dat lek gebruik te kunnen maken. Een firewall kan dit detecteren. Dan wordt op de firewall een "virtuele patch" geïnstalleerd om misbruik van beveiligingslekken elders te voorkomen.

Virtual patching is ook een oplossing voor beveiligingsproblemen waarvoor de verantwoordelijke leverancier nog geen patch heeft uitgegeven. De leverancier van de firewall kan hierop vooruit lopen, waardoor men toch tegen misbruik van aanwezige beveiligingslekken beschermd is.

Soms wordt bij systemen met redundante besturingen één besturing uit bedrijf genomen om te patchen, terwijl de andere besturing in bedrijf blijft en productie dus door kan gaan. De redenering is dan dat dit een slim gebruik is van de redundante mogelijkheden. Echter, op deze manier is het

systeem dus enige tijd niet meer redundant! De redundantie is nodig voor de bedrijfszekerheid, die nu dus niet meer gegarandeerd kan worden.

8.2.5 HOEVEEL SOFTWARE IS ER TE PATCHEN

Bij patchen wordt vaak alleen gedacht aan PC's. Uiteraard worden hiervoor (door Microsoft) patches uitgeleverd, elke tweede dinsdag van de maand. Maar Microsoft is niet verantwoordelijk voor alle software op een PC. Er is nog veel meer: andere browsers, browser plugin software, PDF lezers, media players, printer software, applicatiesoftware, database pakketten, antivirus engineering-software, SCADA pakketten, programmeertalen (zoals Java), de BIOS, disk drivers, USB drivers, etc. Al deze leveranciers kunnen hun eigen patches uitgeven, in een eigen cyclus, of soms helemaal niet. Het komt in de PC-wereld ook voor dat softwarepakketten zélf controleren of er een nieuwere versie beschikbaar is ("auto-update"), maar dat is zeker nog niet overal gebruikelijk.

SCADA
Java

Naast PC's is er in nog veel apparatuur software aanwezig: printers, NAS (Network Attached Storage), routers, switches, WiFi access points, telefoons, monitors, UPS'en, PLC's, remote I/O, frequentie omvormers, meetapparatuur, servo's, database servers, etc. (misschien kunnen we ons beter afvragen in welke apparatuur nog géén software zit). Ook hier is er soms noodzaak tot het installeren van patches (veelal in de vorm van een complete update). Aangezien PC's steeds beter beveiligd zijn, verleggen hackers hun aandacht steeds meer naar de 'zwakkere broeders' op een netwerk en met succes. Zelfs gerenommeerde leveranciers op dit gebied zijn de afgelopen jaren op deze wijze verrast.

8.3 WAT ZIT WAAR EN HOE WERKT HET?

In een ideale wereld is precies bekend hoe een industrieel netwerk er uit ziet, wie erop aangesloten is, wat iedereen doet, wie met wie communiceert, welke software overal op staat, waar de koppelingen naar buiten liggen, wie waarvoor verantwoordelijk is en dat iedereen weet hoe met cybersecurity om te gaan.

De praktijk is vaak net even anders:

- Het netwerk is door de jaren heen gegroeid, er is geen (actuele) documentatie meer en problemen worden opgelost door "volg de kabel" en zie daar dan weer verder;
- Datastromen op het netwerk zijn niet bekend: wie communiceert met wie, hoeveel data, waarom eigenlijk?
- Diverse generaties besturingen van verschillende leveranciers, gekoppeld aan veel soorten PC's werkend op diverse (oude en nieuwe) Windows varianten met allemaal verschillende instellingen;
- Onderhoud wordt uitgevoerd als er problemen zijn;
- Door bezuinigingen op personeel is er een hoge werklast, zodat niet voldoende afstand kan worden genomen van de dagelijkse problemen om zodoende een structurele verbetering door te kunnen voeren;
- Klanten en/of toeleveranciers hebben remote access mogelijkheden; firewalls (indien al aanwezig) staan waarschijnlijk wijd open;
- Omdat er geen documentatie is, kunnen wijzigingen niet uitgevoerd worden omdat niet duidelijk is wat de consequenties zijn;
- Cybersecurity heeft geen prioriteit, "er is nog nooit iets gebeurd".

In zo'n situatie is het niet mogelijk om een goede beveiliging te krijgen. De eerste stap moet daarom altijd zijn: inventariseer. De SANS Top-20 (*zie hoofdstuk 7.2*) en ISA-99 / IEC 62443 (*zie hoofdstuk 7.4*) beginnen hier dan ook mee.

ISA-99
IEC 62443

Als bekend is welke apparatuur er aanwezig is en welke software daar bij hoort, kan een assessment gedaan worden naar de mogelijke bedreigingen voor bepaalde zwaktes. Niet elke zwakte is automatisch een probleem; aan een zwakte zonder (interne of externe) bedreiging hoeft niets gedaan te worden. Verder is er natuurlijk nog de vraag "is het kosteneffectief". Als misbruik van een zwakte maar voor € 1000 schade toebrengt maar het aanpakken ervan kost een veelvoud hiervan, dan is het misschien effectiever om niets te

doen. Hiervoor zijn geen standaard regels te geven, dit is per bedrijf en zelfs per systeem anders.

Ook hoe een bepaalde zwakte aangepakt wordt, is niet in een standaard regel te beschrijven. De oplossing hoeft niet altijd iets technisch te zijn; veel is in procedures te regelen. Standaarden zoals ISA-99 / IEC 62443 (en vele andere) helpen bij het uitvoeren van de bovengenoemde stappen en het maken van de juiste afwegingen. Er is geen enkele reden om zelf het wiel opnieuw uit te vinden.

ISA-99
IEC 62443

8.4 TOT SLOT: HOUD HET HOOFD KOEL

Sinds het Stuxnet virus (*zie hoofdstuk 4*), is er veel meer aandacht voor industriële cybersecurity. En die aandacht is er dan in zodanige mate dat veel van wat fout gaat 'natuurlijk' de schuld is van een virus (gemaakt door de Russen, de Chinezen, al-Qaida, etc.). Allerlei instanties zonder kennis van zaken beginnen zich er dan ook mee te bemoeien en het hek is van de dam. Dit komt ook omdat aan hackers vaak een bovengemiddelde intelligentie wordt toebedacht en alles wat

Stuxnet
Virus

dan niet normaal verklaard kan worden is dus ‘opeens’ een hack. Als er dan ook nog geen enkel bewijs van een virus gevonden kan worden dan is er ‘dus’ sprake van een supervirus.

Een voorbeeld hiervan vond in 2011 plaats bij een waterleidingbedrijf in de VS. Hier ging een keer een waterpomp onverwacht kapot. Vrij kort daarna trof men in de logbestanden aan dat iemand vanuit Rusland had ingelogd op het netwerk van het waterleidingbedrijf. Nu koppelde iemand beide zaken aan elkaar: een hacker heeft vanuit Rusland de waterpomp op afstand vernield. De bal ging aan het rollen: experts claimden “ik zei het toch!”, de cybersecurity-industrie stond op zijn achterste benen over de zwakke beveiliging van de drinkwatervoorziening, de politie stelde een onderzoek in, de FBI deed dat ook nog eens, er was veel media-aandacht, etc. Er kon echter geen spoor van malware gevonden worden.

Vrij snel daarna kwam de aap uit de mouw. Het waterleidingbedrijf had zijn systeemintegrator gebeld om eens naar de besturing te kijken. De systeemintegrator had een medewerker hierover gebeld. Deze bleek in Rusland op vakantie te zijn, maar was dankzij zijn GSM gewoon bereikbaar. Via een internetaansluiting is toen op afstand ingelogd en deze actie kwam dus in het logboek te staan.

Al met al was de hele waterpomp ‘hack’ dus een storm in een glas water. Blijkbaar kunnen waterpompen ook gewoon uit zichzelf kapot gaan, zo was de conclusie. Daarna werd nog meer tijd verspild aan het zwartepieten tussen allerlei instanties, experts, de politie, etc.

Laat je dus niet ‘gek’ maken en houd het hoofd koel maar onderschat de gevaren van cybersecurity niet en inventariseer de risico’s voor elke installatie.

Phoenix Contact en andere leveranciers en bedrijven die gespecialiseerd zijn in cybersecurity bieden u graag een helpende hand.

WOORDENBOEK

A

AES

Advanced Encryption Standard

Wiskundig algoritme voor encryptie van data, dat onder andere gebruikt wordt in WiFi. Het algoritme is ontwikkeld door de Belgische wiskundigen Vincent Rijmen en Johan Daemen, als opvolger van het oudere algoritme genaamd DES (Data Encryption Standard) waarvan de beveiliging doorbroken was. Het is ook wel bekend onder de benaming Rijndael. AES is nog steeds niet gekraakt, hoewel daar (uiteraard) wel onderzoek naar wordt verricht; in 2011 werd bekend dat dankzij een wiskundig slimmigheidje een kraakpoging 4x zo snel als eerst zou kunnen verlopen. Hiervoor is aan rekentijd dan nog steeds meerdere malen de leeftijd van het heelal nodig, zodat dit in de praktijk geen verschil maakt.

In WiFi is het de opvolger van het aan alle kanten kraakbare ***WEP*** algoritme. In de norm IEEE 802.11i is AES onder de benaming *WPA2* geïntroduceerd.

AIR GAP

Beveiligingsmethode waarbij ervoor gezorgd wordt dat er géén netwerkverbinding bestaat tussen het te beveiligen systeem en het bedrijfsnetwerk en/of internet, m.a.w. er zit een 'gat'. Dat geldt niet alleen voor bekabelde netwerken, maar ook voor draadloze netwerken.

Over de effectiviteit van air gaps bestaat veel twijfel. Aangezien toch vaak datatransport van/naar het beveiligde systeem nodig is, worden datadragers zoals USB-sticks, CD's en vroeger floppies ingezet. Hierop kan ook malware staan, zodat een infectie nog steeds mogelijk is. Tegenstanders van air gaps claimen dan ook dat het een vals gevoel van veiligheid geeft, waardoor vaak afgezien wordt van additionele beveiligingsmethodes en het eindresultaat is dat men eindigt met een zeer zwak (of helemaal niet) beveiligd systeem.

APT

Advanced Persistant Threat

Benaming voor een type malware dat qua werking en complexiteit uitstijgt boven de 'gemiddelde' malware. In de loop der jaren is de term erg aan inflatie onderhevig geraakt, zodat alle nieuwe of nog onbegrepen malware al snel zo genoemd wordt.

ARP

Address Resolution Protocol

Eenvoudig netwerkprotocol dat als onderdeel van TCP/IP werkt en er voor zorg draagt dat voor elk uitgaand IP-netwerkbericht het bij het IP-adres behorende Ethernet ***MAC-adres*** wordt bepaald. Een TCP/IP applicatie hoeft dan zelf niets te weten van het onderliggende netwerk; het opgeven van het IP-adres van de bestemming voor een netwerkbericht is voldoende. ARP houdt de berekende informatie bij in de zgn. "ARP tabel", die op Unix-systemen en Windows-PC's met het commando "arp –a" op te vragen is.

ARP SPOOFING

Methode om het ***ARP***-protocol om de tuin te leiden, door ARP-netwerkberichten te sturen met valse informatie hierin, namelijk een ander MAC-adres dan eigenlijk bij een IP-adres hoort. Netwerkberichten naar dat IP-adres worden dan naar iemand anders gestuurd, die dan in die netwerkberichten kan meekijken zonder dat de oorspronkelijke zender dat in de gaten heeft.

AUTHENTICATIE

Procedure waarmee vastgesteld wordt of een gebruiker (of een apparaat) werkelijk is wie men claimt te zijn. De authenticatie kan plaatsvinden aan de hand van: iets dat men is (vingerafdruk, IRIS-scan, gezichtkenmerken) en/of iets dat men weet (wachtwoord, PIN-code, geheime zin) en/of iets dat men bezit (certificaat, identiteitsbewijs, telefoonnummer, sleutel, smartcard, e-mailadres).

Authenticatie via slechts één van deze drie kenmerken is zwak; daarom wordt vaak 2-factor authenticatie gebruikt in digitale omgevingen.

B

BABBLING NODE, BABBLING IDIOT

Deelnemer in een netwerk die continu een transmissie uitvoert, doorgaans door een probleem met de elektronica. Een babbling idiot kan het gehele netwerk doen stilvallen. Bepaalde netwerken beschikken over speciale elektronica om dit te voorkomen. Ook via software kan een deelnemer zich als babbling idiot gaan gedragen, waardoor geen bandbreedte voor anderen meer over is.

BACKCHANNEL

Een backchannel is een secundair communicatiekanaal dat parallel werkt aan het primaire communicatiekanaal. In de context van cybersecurity is dit meestal niet gewenst, omdat de beschikbaarheid / aanwezigheid van een backchannel veelal geheel onopgemerkt blijft en zodoende malware op een systeem binnengebracht kan worden. Backchannels worden vaak automatisch gestart door een e-mail te sturen met een besmette attachment erbij; als deze geopend wordt of geactiveerd, opent het backchannel (om het attachment op te halen) en kan elders malware opgehaald worden c.q. data opgestuurd worden. Omdat dit 'achter' de ***firewall*** geïnitieerd wordt, kan deze het backchannel niet blokkeren; het is immers niet te onderscheiden van een door de gebruiker gestarte actie (zoals het lezen van een valide webpagina).

BACKDOOR

Een in een apparaat ingebouwde faciliteit om toegang tot dat systeem te krijgen buiten de reguliere mogelijkheden om. Dit wordt vaak door leveranciers ingebouwd om eenvoudig bij klanten, diagnose op afstand te kunnen uitvoeren, om fabrieksinstellingen te programmeren direct na productie of om programmeurs toegang te geven tot

testfuncties. Dit zijn vaak zeer krachtige mogelijkheden die, indien door onbevoegden gebruikt, het functioneren van het apparaat kunnen beïnvloeden of het zelfs geheel kunnen laten uitvallen.

Alhoewel dit soort backdoors toegevoegd zijn om valide redenen, is het probleem dat ze veelal onbekend zijn bij de eindgebruikers en derhalve ook niet opgenomen zijn in de reguliere beveiligingsmaatregelen. Verder hebben dit soort backdoors vaak zwakke wachtwoorden (of helemaal geen), die soms ook niet te wijzigen zijn en dus voor alle apparaten van hetzelfde type wereldwijd hetzelfde zijn. Het bekend worden van zo'n vast wachtwoord is dus desastreus.

Omdat backdoors vaak in het bedrijfssysteem van een apparaat zijn ingebouwd, kunnen ze niet gedetecteerd worden en ook niet (snel) verwijderd worden. Het is ook mogelijk dat backdoors in chips ingebouwd kunnen worden.

BLACKLISTING

Methode waarmee toegang wordt geweigerd aan iedereen die op de "zwarte lijst" staat. Dit kan bijvoorbeeld zijn op basis van naam, maar ook op soort protocol, netwerkadres, etc. Wie / wat niet op de lijst staat, wordt toegelaten. Het nadeel van blacklisting is dat de lijst vaak snel achterhaald is. De tegenovergestelde methode is ***whitelisting***.

BLUE TEAM

Benaming voor het team dat in een cursus of ***penetratietest*** de verdedigende rol heeft. Hier tegenover staat het ***red team***, dat moet proberen een systeem binnen te komen.

BOT

Deelnemer (onvrijwillig!) in een ***botnet***. Een andere benaming hiervoor is: ***zombie***.

BOTNET

Robot network

Een groep computers (***bots***) die collectief op afstand bestuurd wordt vanuit een ***Command & Control Center***. Een botnet kan uit tienduizenden tot meer dan honderdduizend bots / zombies bestaan, verspreid over de hele wereld. Op afstand kan het botnet ingezet worden voor het massaal sturen van e-mails (spam) of een ***Denial Of Service*** aanval op een website, die overbelast raakt door het enorme aantal bezoekers. Een systeem wordt veelal onvrijwillig deel van een botnet, na installatie van malware die via besmette e-mails of websites geïnstalleerd wordt. De eigenaar van het systeem merkt er vaak niets van.

Omdat de feitelijke beheerder van het botnet op afstand actief is, is het vinden van deze personen erg lastig. Bestrijding van een botnet wordt vaak gestart door het uit de lucht halen van het command & control center, gevolgd door het opschonen van de besmette PC's. Omdat het over zeer veel systemen gaat, is dat erg lastig. Systemen op afstand opschonen, zonder kennis van de eigenaar, stuit op veel juridische bezwaren. Wel kan de eigenaar een boodschap getoond worden dat zijn systeem besmet is, met een verzoek om het op te schonen. Dit wordt echter ook wel eens door malware zelf gemeld, om zo de gebruiker mee te laten helpen aan het installeren van nog meer malware. *Zie ook:* ***ransomware, scareware***.

BRUTE FORCE AANVAL

Methode voor het kraken van wachtwoorden, pincodes, etc. door ze eenvoudigweg allemaal uit te proberen, bijvoorbeeld: aaaaaa, aaaaab, aaaaac, ... aaaaba, aaaabb, ... zzzzzy, zzzzzz voor 6-letterige wachtwoorden. Met moderne processoren kunnen al enkele miljarden wachtwoorden per seconde worden doorgerekend.

Eén methode voor software om brute force aanvallen te frusteren is om na het gebruik van een verkeerd wachtwoord een bepaalde wachttijd in acht te nemen voordat

een nieuw wachtwoord gegeven mag worden, bijvoorbeeld, 1, 2, 5, 10, 20 .... seconden. Ook kan een limiet gesteld worden aan het maximale aantal foute pogingen, bijvoorbeeld: 3x een verkeerde pincode invoeren leidt tot blokkade van een pinpas.

Brute force op wachtwoorden die gecodeerd zijn opgeslagen in bestanden zijn vaak wel eenvoudig mogelijk, omdat geen externe software gebruikt hoeft te worden die zegt of een wachtwoord klopt of niet. Dit wordt vaak gebruikt om gebruikersadministraties van websites te kraken. De enige mogelijkheid om een brute force aanval te weerstaan is om zodanig lange wachtwoorden te gebruiken dat de brute force aanval te veel rekentijd nodig heeft. Doordat de afgelopen decennia rekenkracht erg goedkoop geworden is, zijn steeds langere wachtwoorden nodig; waar vroeger wachtwoorden van 6 karakters nog veilig waren, wordt tegenwoordig al aangeraden minstens 10 à 12 karakters te gebruiken.

Ook het gebruik van andere karakters dan enkel a-z of A-Z maakt wachtwoorden complexer en een brute force aanval moeilijker. Dit is de reden dat bij de keuze van een wachtwoord vaak wordt afgedwongen dat er een cijfer, een leesteken en een mix van hoofdletters en kleine letters gebruikt wordt.

BUMA/STEMRA VIRUS

Zie: ***politievirus***.

BUNDESTROJANER

Door de Duitse politie ontwikkelde software, die op de PC van een verdachte kan worden geïnstalleerd. Met de software kunnen Skype-gesprekken worden afgeluisterd, op afstand een webcam of microfoon worden ingeschakeld, toetsaanslagen worden opgeslagen, schermafdrukken gemaakt worden, aldus een onderzoek van de Duitse Chaos Computer Club.

C

CAFE LATTE AANVAL

In 2007 ontdekte methode om op een zodanig snelle manier het wachtwoord van een met ***WEP*** beveiligd WiFi-netwerk te achterhalen, dat het gedaan kan worden vóórdat de genoemde kop koffie geconsumeerd is.

C&C CENTER

Zie: ***Command & Control Center*** *en* ***Botnet***.

CERT

Computer Emergency Response Team

Team dat in een organisatie opgesteld staat om beveiligingsincidenten af te handelen, zowel komende van buiten, van binnen of via verkochte producten. Een CERT kan bestaan binnen elke willekeurige organisatie, bijvoorbeeld een overheid, maar ook een bedrijf kan een CERT hebben. Een CERT is een soort van "digitale brandweer" in een organisatie.

De eerste CERT ooit was die van de Carnegie-Mellon Universiteit, die de naam CERT inmiddels als handelskenmerk (TM) heeft laten registreren. Als alternatief wordt daarom ook wel de benaming ***CSIRT*** (Computer Security Incident Response Team) gebruikt, die toch minder bekend is en gebruikt wordt dan CERT. Een complete lijst van CERT's is te vinden op: www.cert.org/csirts/cert_authorized.html.

De Belgische nationale CERT is www.cert.be; de Nederlandse is www.ncsc.nl (voorheen: GovCert). Bedrijven hebben soms ook een eigen CERT.

COMMAND & CONTROL CENTER

Een computer die op internet de besturing van een ***botnet*** verzorgt, zoals daar achtergelaten door de botnet beheerder. De geïnfecteerde systemen in het botnet zoeken regelmatig contact met het C&C Center voor het ontvangen van verdere instructies. Een effectieve

manier om botnets stil te leggen is het oprollen van het C&C Center (uiteraard moeten daarna de geïnfecteerde systemen ook nog worden opgeschoond).

CONFICKER

Naam van een zeer beruchte ***worm***, die zich verspreidde op Windows computers dankzij een beveiligingsfout. De eerste versie is in 2008 ontdekt; later volgden nog 4 nieuwere versies. Omdat zeer geavanceerde technieken werden gebruikt voor de infectie en verspreiding en de auteurs nieuwe versies lanceerden, was het zeer moeilijk om Conficker te bestrijden; in 2013 was de worm nog steeds actief.

COOKIE

Een door een website op een computer achtergelaten bestand waarin willekeurige informatie kan worden opgeslagen, die door de website weer gebruikt kan worden als de gebruiker die website opnieuw bezoekt. Denk daarbij aan gebruikersnaam en/of wachtwoord, maar ook voorkeursinstellingen, bezochte webpagina's, etc. Vanuit oogpunt van marketing is dit zeer interessante informatie, die verzameld kan worden zonder dat de gebruiker van een PC weet dat dit gebeurt, wat er dan wel allemaal aan informatie wordt verzameld en aan wie dat wordt verzonden. Vanuit het oogpunt van beveiliging is het opslaan van gebruikersnamen en wachtwoorden in cookies zeer gevaarlijk, ook al is het automatisch inloggen op een website voor een gebruiker erg eenvoudig. Goed ontworpen websites doen dit dan ook niet.

In 2012 is het daarom in Europa verplicht geworden dat een website alleen een cookie mag plaatsen na toestemming van de gebruiker, tenzij de cookie nodig is om technische redenen. Wie geen cookies wil kan dit in moderne webbrowsers ook stoppen, maar sommige websites kunnen dan niet meer functioneren. Ook is het mogelijk om bij afsluiten van de webbrowser alle cookies te verwijderen. Virusscanners kunnen dit ook doen.

Aangezien websites graag met cookies werken, is er een continue strijd tussen diegenen die cookies willen plaatsen en de gebruikers die ze weer weg willen hebben. In 2010 kwam het bestaan van een zogenaamd "Evercookie" aan het licht, die extreem moeilijk te verwijderen zou zijn omdat de informatie redundant op een PC wordt opgeslagen. Ook al zou een browser na afloop alle eigen cookies verwijderen, dan nog zijn kopieën ervan elders op de PC te gebruiken om na herstart van de browser alle cookies weer te herstellen.

COMPENSATING CONTROL

Secundaire beveiligingsmaatregel die ingevoerd wordt omdat een (technische of organisatorische) zwakte elders in het systeem niet verwijderd kan worden of zelf afdoende beveiligd kan worden.

CSIRT

Computer Security Incident Response Team

Zie: ***CERT***

CYBERWAR

Vorm van oorlogsvoering waarbij de tegenstander wordt aangevallen door zijn apparatuur, infrastructuur (communicatie, energie, water, ziekenhuizen, vliegvelden enz.) en IT-systemen met malware te beïnvloeden, waardoor deze verminderd beschikbaar zijn of helemaal uitvallen of andere schade aanrichten.

Aangezien moderne staten sterk afhankelijk zijn van geautomatiseerde systemen, is er steeds meer aandacht voor cyberwar, niet alleen voor de offensieve mogelijkheden, maar uiteraard ook voor de defensie hiertegen.

Een 'voordeel' van cyberaanvallen op andere landen is dat ze nauwelijks te detecteren zijn en dus ook in vredestijd uitgevoerd kunnen worden zonder dat de uitvoerder ervan bekend hoeft te zijn. ***Stuxnet*** wordt soms gezien als een vorm van cyberwar, waardoor de nucleaire ambities van Iran fors vertraagd zijn.

D

DAMN VULNERABLE LINUX

Versie van Linux die speciaal ontwikkeld is om eenvoudig hackbaar te zijn. Deze versie bevat expres verouderde software of is slecht c.q. verkeerd geconfigureerd. Het kan gebruikt worden voor opleidingen of voor gebruik in ***honeypots***.

DATADIODE

Zie: ***netwerkdiode***.

DEEP PACKET INSPECTION (DPI)

Methode van controle van netwerkberichten door een firewall, waarbij niet (zoals gebruikelijk) alleen de administratieve velden van een TCP/IP netwerkbericht worden gecontroleerd, maar ook de gebruikersdata in die netwerkberichten. Hiermee kan het gebruik van bepaalde protocollen (en bijbehorende applicaties) worden geblokkeerd, toegang tot bepaalde websites worden tegengegaan, tekst van e-mails gescand, etc. In een industriële toepassing kan bijvoorbeeld het lezen van setpoints van procesvariabelen wel worden toegestaan, maar het wijzigen ervan niet.

DEFENSE IN DEPTH

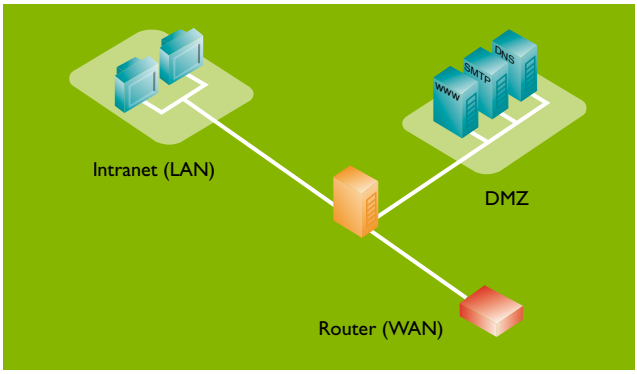
Methode van beveiliging van netwerken tegen hackers en virussen, waarbij niet wordt vertrouwd op één verdedigingsmethode, maar meerdere achter elkaar. Het idee hierbij is dat geen enkel systeem onkwetsbaar is te krijgen tegen alle mogelijke aanvallen. Ook al kan een aanvaller één (of enkele) verdedigingsmechanismen doorbreken, dan zijn er nog andere verdedigingsmechanismen actief die hem dan toch nog tegen kunnen houden.

DEMILITARIZED ZONE (DMZ)

Speciaal deel van een netwerk dat als intermediair fungeert tussen internet en een beveiligd intern netwerk. Het wordt ook wel een ‘extranet’ of ‘perimeter

network' genoemd. In de DMZ worden die systemen aangesloten die zowel van buitenaf als van binnenuit te benaderen moeten zijn, zoals bijvoorbeeld een webserver, een e-mailserver of een bestandsserver. Toegang tot internet vanuit het interne netwerk kan ook via de DMZ lopen, als daar een "proxy server" wordt geïnstalleerd.

De DMZ wordt op het interne en externe netwerk gekoppeld via firewalls; hiervoor zijn diverse oplossingen mogelijk. De onderstaande afbeelding toont een oplossing met twee firewalls; de firewall aan internet laat alleen verkeer toe naar de DMZ (en retour). De tweede firewall laat alleen verkeer vanuit het intranet van/naar de DMZ toe.



◀ netwerkarchitectuur met een DMZ *(bron: Wikipedia)*.

DENIAL OF SERVICE (DOS)

Een aanval op een systeem waardoor het niet meer in staat is om zijn gebruikelijke functie uit te voeren.

In tegenstelling tot andere vormen van aanvallen op systemen raakt het aangevallen systeem niet permanent beschadigd; is de DoS-aanval afgelopen (of afgeslagen) dan staat de volledige functionaliteit weer ter beschikking.

Een eenvoudige manier om een DoS-aanval uit te voeren is om vanaf meerdere systemen tegelijk heel veel netwerkberichten te sturen naar dezelfde bestemming.

De processor moet hierop aan al deze netwerkberichten toch enige aandacht besteden (al is het maar om ze verder te negeren), maar dat kost uiteraard CPU-tijd. Het gevolg is dan dat de processor al zijn tijd hieraan moet besteden, zodat er geen tijd meer overblijft voor nuttige taken. Ook is het mogelijk dat het systeem crasht door overbelasting.

DoS-aanvallen op webservers komen vaak voor, soms gedreven door hacktivisten om aandacht te vestigen op maatschappelijk actuele thema's. Aangezien webservers van grote websites goed in staat zijn om veel netwerkverkeer af te handelen, moet er ook heel veel netwerkverkeer gegenereerd worden om enig effect te hebben. Hiervoor wordt dan een ***botnet*** of zombie-netwerk ingezet, zodat eenvoudig tienduizenden PC's aangestuurd kunnen worden om tegelijk dezelfde website te bezoeken.

Een DoS kan ook onbedoeld optreden als een Ethernetnetwerkkaart defect raakt of bij verkeerd geconfigureerde netwerken waarbij de netwerktelegrammen dan kunnen gaan "rondzingen".

DMZ

Zie: ***Demilitarized Zone***

DORIFEL

Naam van een virus dat medio 2012 ontdekt werd en veel Nederlandse gemeentes en overheidsinstellingen infecteerde. Het virus verminkte documenten die het op de getroffen PC vond. Een latere versie deed dit niet meer, maar blokkeerde de computer zogezegd omdat de ***Buma/Stemra*** had gedetecteerd dat er illegale bestanden op de PC zouden staan; na betaling van 100 Euro werd de PC weer vrijgegeven.

DOS

Zie: ***Denial of Service***

DPI

Zie: ***Deep Packet Inspection***

DRIVE-BY ATTACK

Aanval op het computersysteem van een gebruiker die plaatsvindt enkel en alleen door het bekijken van een webpagina. Veel webpagina's laten advertenties zien die elders worden opgevraagd; als zo'n advertentie besmet is met malware kunnen zelfs websites met een goede reputatie gevaarlijk zijn.

DROPZONE

Computer waarop via malware gestolen informatie (tijdelijk) wordt opgeslagen. De eigenaar van zo'n computer is zich waarschijnlijk onbewust van het gebruik ervan.

DUQU

Een ***worm*** die in 2011 ontdekt werd en die veel karakteristieken van ***Stuxnet*** had, waardoor er in de industriële wereld veel aandacht aan werd besteed. In tegenstelling tot Stuxnet deed Duqu echter niets met industriële besturingen, maar leek alleen maar op zoek te gaan naar bepaalde documenten, om die vervolgens te kopieren naar een server ergens in de wereld. Ook kon het screendumps maken, toetsaanslagen opslaan en allerlei informatie over de lokale computer verzamelen en dit wegsturen. Vanwege deze datahonger wordt gespeculeerd dat Duqu op zoek was informatie over een nog in de toekomst aan te vallen systeem of organisatie.

E

EVIL MAID AANVAL

Benaming voor een methode om zelfs op een laptop, waar alle data gecodeerd op de harde schijf is opgeslagen, toch deze data te kunnen decoderen. Het voorbeeldscenario is dat een laptop op een hotelkamer is achtergelaten; waarna de aanvaller met de sleutel van het kamermeisje binnenkomt en dan een speciaal opstart-

programma (“bootloader”) installeert – dit is op de meeste laptops eenvoudig mogelijk. Als de laptop de volgende keer door de eigenaar opgestart wordt, wordt het wachtwoord afgetapt. De aanvaller komt later nog een keer terug en kan dan de data op de harde schijf decoderen en kopiëren. Eventueel kan daarna de speciaal geïnstalleerde software weer verwijderd worden, zodat op de laptop geen enkel spoor van de aanval meer te vinden is.

Uiteraard is een “Evil Maid” aanval ook mogelijk buiten hotelkamers; ook thuis of in een bedrijf. Encryptie van data helpt dus wel tegen diefstal van een laptop, maar niet tegen het specifieke hier besproken scenario, waarbij fysieke toegang tot de laptop mogelijk is.

EXPLOIT

Software die speciaal geschreven is om van een beveiligingslek misbruik te maken. Vroeger werd een virus, worm of Trojan gemaakt voor één exploit. Tegenwoordig zien we ook malware (zoals ***Stuxnet***, ***Duqu*** en Shamoon) die een heel scala aan exploits kan bevatten, om de kans op een succesvolle inbraak zo groot mogelijk te maken.

EXPLOIT KIT

Softwarepakket dat door hackers verkocht word en waarmee iemand zelf eenvoudig een eigen virus kan maken. Net zoals in de reguliere software-industrie kan er een helpdesk zijn, worden regelmatig nieuwe versies geleverd (bijvoorbeeld om beter bestand te zijn tegen de nieuwste virusscanners) en kunnen speciale wensen tegen betaling geprogrammeerd worden.

F

FALSE NEGATIVE, FALSE POSITIVE

Een melding van een ***firewall***, een ***intrusion detection system*** of een ***virusscanner*** die niet klopt. Een “false

negative" is een aanval of malware die niet correct gedetecteerd wordt (gemist wordt dus). Elke "false negative" is dus gevaarlijk, aangezien het systeem niet doet waar het voor aangeschaft is. Een "false positive" is een onterechte melding over een aanval of over malware die er niet is. Als er teveel "false positive" meldingen gegeven worden, neemt het vertrouwen in het systeem af en zal er steeds langzamer (of helemaal niet meer) op meldingen gereageerd worden.

FIREWALL

Een systeem dat enerzijds aan internet en anderzijds aan het (thuis, bedrijfs)-LAN is aangesloten en dat alle heen- en weergaande netwerkberichten controleert. Het kan ook geïmplementeerd zijn als softwarepakket dat op een PC geïnstalleerd moet worden (vaak als onderdeel van een virusscanner); het controleert dan alle inkomende netwerkverkeer zodra het op een netwerkpoort binnenkomt en controleert ook alle uitgaande netwerkverkeer.

De firewall moet voorkomen dat van buitenaf opererende hackers toegang krijgen tot het eigen netwerk en de daarop aangesloten apparatuur. Tevens kan het controleren of van binnen het bedrijf uit contact wordt gezocht met bepaalde websites of bepaalde servers en kan het controle uitoefenen op de inhoud van het netwerkverkeer. Een firewallsoftwarepakket moet niet noodzakelijk op een aparte computer draaien; indien het op de eigen PC geïnstalleerd wordt, schermt het alleen de eigen PC af. De zwakte van een firewall is dat alle inbraakpogingen die achter de firewall plaatsvinden, niet gedetecteerd worden. Met de opkomst van toegangsstations (access points) voor draadloos Ethernet, die zeer snel aan een LAN te koppelen zijn of in een laptop ingebouwd zijn, is een achterdeurtje zo geopend. *Zie ook:* ***stateful firewall.***

FOREVER DAY

Benaming voor een beveiligingsprobleem dat nooit (meer) opgelost gaat worden, ook al is het bekend bij de

leverancier. Dit gebeurt dan vooral bij software waarvan de commerciële levensduur overschreden is of waarvoor geen ondersteuning meer geleverd wordt. Bijvoorbeeld, Microsoft lost geen beveiligingsproblemen meer op voor Windows NT, Windows 2000 en XP versies.

FTP

File Transfer Protocol

Protocol uit de TCP/IP familie waarmee het mogelijk is om bestanden over te sturen naar andere systemen of om bestanden elders op te halen. Gebruik van FTP wordt voor veel toepassingen afgeraden omdat wachtwoorden in leesbare tekst worden overgestuurd.

FUZZER

Software die willekeurige netwerkberichten met willekeurige inhoud stuurt naar deelnemers op een netwerk, met de bedoeling om de protocolafhandelingssoftware op die deelnemers te laten stoppen of het gehele systeem te laten crashen. Hierdoor is zo'n deelnemer niet meer via het netwerk te bereiken en kan dus ook niet meer functioneren in een groter geheel (machine, productielijn, etc.).

Heel veel software controleert niet goed wat er in een netwerkbericht staat. Dat is normaliter nooit een probleem omdat in normale omstandigheden alleen netwerkberichten met een valide inhoud verstuurd worden.

H

HACKTIVISME

(samenvoeging van "hacken" en "activisme"). Een vorm van (maatschappelijk) protest of het uitdragen van een politieke boodschap, die wordt uitgevoerd door websites van bepaalde bedrijven of instanties aan te vallen, te modificeren of te laten stoppen enz. Dit geeft vaak de nodige aandacht in de pers en zodoende kan de boodschap van de activisten worden uitgedragen.

HASH, HASHING

Een cryptografisch algoritme dat een digitale vingerafdruk uitrekent van een hoeveelheid elektronische data. Deze "hash" is uniek voor die data. Elke wijziging aan die data, hoe klein ook, leidt tot een geheel andere hash. Daarmee is dus te zien of de data gewijzigd is of niet.

Een hele primitieve vorm van een hash is een controlecijfer zoals in een negenproef; twee voorbeelden hiervan zijn het laatste cijfer bij ISBN-codes (op boeken) en van nummers van bankbiljetten of bankrekeningen.

Hashing is dus géén vorm van encryptie: de originele data is niet meer terug te rekenen. Een hash heeft een bepaalde lengte in bits, bijvoorbeeld 256. Hoe groter het aantal bits, des te veiliger is de berekende hash. Bekende hash-algoritmes zijn o.a. MD5 en diverse uit de ***SHA*** familie.

HONEYPOT

Een systeem dat speciaal bedoeld is om hackers te lokken en hun activiteiten te monitoren. Het kan bestaan uit een standaard systeem waarvan het beveiligingsniveau met opzet verlaagd is of uit speciale software die een bepaald systeem simuleert. Het voordeel van deze laatste methode is dat de hacker geen echte schade aan kan richten en al zijn acties zeer goed te volgen zijn. Hierdoor kan mogelijk de identiteit of de locatie van de hacker vastgesteld worden. Een (klein) extra voordeel is dat de tijd die de hacker aan de honeypot besteedt, niet meer gebruikt kan worden om een echt systeem aan te vallen.

HUMAN FIREWALL

Concept waarbij de eerste lijn van verdediging van een systeem tegen hackers, wordt uitgevoerd door op het gebied van cybersecurity goed opgeleide werknemers, in plaats van enkel te vertrouwen op technische maatregelen (zoals ***firewalls***). Het gaat hierbij veelal om 'gezond verstand' maatregelen. Enkele voorbeelden: geen wacht-

woorden via de telefoon, geen e-mails openen van onbekenden, geen gevonden USB-sticks gebruiken, etc.

I

IDS

Zie: ***Intrusion Detection System***

IEC 62443

De opvolger van de ***ISA-99*** standaard, uitgebreid met het document "Security Requirements for Vendors" van WIB. Zie ook hoofdstuk 7.

INTRUSION DETECTION SYSTEM (IDS)

Een systeem dat in een netwerk opgesteld staat om inkomende bedreigingen te detecteren, via een analyse op afgetapte netwerkberichten. Indien een bedreiging wordt gezien dan wordt deze gerapporteerd.

ISA-99

Standaard van de International Society of Automation (www.isa.org), speciaal gericht op cybersecurity voor procesinstallaties. De opvolger hiervan is ***IEC 62443.***

ISAC

Information Sharing & Analysis Centre

Werkgroepen waarin bedrijven of instellingen, die in dezelfde sector van de industrie of de maatschappij actief zijn, kennis en ervaringen delen over cybersecurity en andere beveiligingszaken. Deelname aan een ISAC is vrijwillig maar niet vrijblijvend (dus niet enkel informatie komen halen, maar ook brengen). Kwetsbaarheden kunnen op deze manier vroegtijdig worden gesignaleerd en met elkaar gedeeld. Organisaties kunnen op deze manier hun weerbaarheid vergroten. Omdat vaak gevoelige informatie wordt gedeeld (ook met concurrenten), werkt een ISAC op basis van vertrouwen; alleen als dat van te voren is aangegeven mag informatie verspreid worden.

In Nederland bestaan er 11 ISAC's (stand medio 2013) voor ziekenhuizen, vliegvelden, banken, waterwinningsbedrijven, havens, de procesindustrie, etc.

J

JAVA

Programmeertaal die in 1997 gelanceerd is door computerleverancier SUN (nu: Oracle) en vanwege de (destijds) nieuwe ***sandbox*** technologie geacht werd erg veilig te zijn. Inmiddels is dat anders en de beschikbaarheid van Java op een systeem wordt als een groot risico beschouwd.

Omdat hetzelfde Java-programma kan "lopen" op diverse systemen, kunnen hackers met één variant van hun Java-malware diverse soorten systemen infecteren (bijvoorbeeld Windows, MAC OS en Android).

JUICE JACKING

Aanvalsmethode waarbij misbruik wordt gemaakt van apparatuur die op een USB-poort wordt aangesloten om op te laden. Een USB-poort heeft namelijk ook altijd een netwerkaansluiting en die kan dan gebruikt worden om malware op een apparaat te installeren of er interessante informatie van af te halen (zoals een adresboek, e-mails en bestanden van een mobiele telefoon). Met een ***USB condoom*** is bescherming hiertegen mogelijk.

K

KEYLOGGER

Software of een apparaatje (dat tussen het toetsenbord en de PC wordt geplaatst) dat alle ingevoerde toetsaanslagen opslaat. Op deze manier kunnen loginnamen en wachtwoorden worden achterhaald.

M

MAC-ADRES

Medium Access Control

Dit is de officiële benaming voor een netwerkadres in Ethernet. Het is 48 bits lang en bestaat uit een 24-bits lang veld dat de leverancier aangeeft en een tweede 24-bits veld dat een volgnummer van de leverancier is. De 48 bits worden door de leverancier in het apparaat geprogrammeerd.

Omdat een MAC-adres wereldwijd uniek is, wordt het vaak als beveiligingsmaatregel gebruikt, door op basis van het MAC-adres toegang tot een netwerk te weigeren of juist toe te staan: zie ***MAC-adres filtering***. Hackers vinden MAC-adressen interessant omdat het iets zegt over het merk, hetgeen weer een opstapje is om meer informatie erover te vinden.

MAC-ADRES FILTERING

Methode van toegangscontrole tot een netwerk (zie ***blacklisting*** en ***whitelisting***) waarbij binnenkomende Ethernetberichten, waarin altijd een afzender ***MAC-adres*** in staat, door te laten of juist te blokkeren op basis van de controle van het MAC-adres.

De waarde van MAC-adres filtering is zeer beperkt, aangezien op de meeste Ethernet-gebaseerde apparaten het MAC-adres gewijzigd kan worden (zie ***MAC spoofing***). Een aanvaller hoeft dus alleen maar te zoeken naar een netwerkbericht met een MAC-adres dat doorgelaten wordt, om daarna dat MAC-adres te misbruiken.

MAC-SPOOFING

Vorm van identiteitsdiefstal op een netwerk, waarbij het MAC-adres van een ander apparaat wordt gebruikt om zich als die ander voor te doen. Op bijna alle Ethernet-gebaseerde apparaten is het in principe mogelijk om het MAC-adres te wijzigen; dit wordt namelijk juist in

de fabricage gebruikt om dat apparaat zijn eigen unieke MAC-adres te geven.

Er zijn ook legitieme redenen om een ingeprogrammeerd MAC-adres te wijzigen in een ander, bijvoorbeeld na vervanging van apparatuur. Een nieuw apparaat heeft per definitie een ander MAC-adres, maar dit kan dan ook wijzigingen in software tot gevolg hebben. Door het nieuwe MAC-adres te vervangen door het oude, is dit niet meer nodig.

MALWARE

Malicious software

Algemene benaming voor kwaadaardige software.

MAN IN THE BROWSER (MITB OF MIB)

Aanvalsmethode waarbij webpagina's, die van een webserver zijn geladen, worden aangepast voordat ze op het scherm getoond worden. Dit is vaak geheel onzichtbaar voor de gebruiker. Het wordt vaak gebruikt om financiële transacties te manipuleren bij internetbankieren, bijvoorbeeld het stiekem invoegen van een overboeking van een extra bedrag naar een speciale bankrekening. Komt dan de webpagina terug waarbij de bank het totale over te boeken saldo geeft, dan wordt de extra overboeking hier weer uitgefilterd en aan de gebruiker het originele saldo toont. Deze geeft dan uiteraard zijn akkoord, onwetend van het feit dat er meer wordt overgeboekt dan bedoeld.

Eén manier om MITB-aanvallen te omzeilen is om delen van de communicatie tussen de gebruiker en de webserver via een ander kanaal dan internet te laten lopen. Bijvoorbeeld, banken doen dit bij internetbankieren door financiële transacties te laten valideren met een via een SMS-bericht ontvangen code.

MAN IN THE MIDDLE (MITM)

Vorm van cyberaanval waarbij een derde apparaat in het communicatiepad tussen twee andere apparaten

geplaatst wordt. Deze "man in the middle" krijgt dan toegang tot alle data die heen-en-weer stroomt. Afluisteren van een conversatie, maar ook injectie van data, is dan mogelijk. Een bekende vorm van MITM aanvallen is bij WiFi-netwerken, waarbij een rogue access point zich voordoet als een ander access point. Zulke apparatuur is op internet voor enkele tientallen Euro's te koop.

METASPLOIT

Naam van een "software framework", een applicatie waarin anderen eenvoudig programmatuur kunnen toevoegen. In dit geval zijn het uitbreidingen om te testen of er beveiligingslekken in andere software aanwezig zijn. Via het Metasploit framework kan dit dan geautomatiseerd worden zonder dat veel kennis bij de gebruiker nodig is. Er is een gratis versie met beperkte mogelijkheden; voor een jaarlijkse licentie van ca. $1500 is de volledige functionaliteit beschikbaar.

Of Metasploit het leven van hackers of beveiligers eenvoudig maakt, verschillen de meningen!

N

NERC

North-American Electric Reliability Corporation

Branchevereniging van Amerikaanse (energie) nutsbedrijven, die een eigen standaard heeft geschreven voor cybersecurity: "NERC CIP" (Critical Infrastructure Protection).

NETSTUMBLER

Bekend freeware programma om de 2,4 GHz band te kunnen monitoren op WiFi-netwerken. Het programma laat o.a. zien welk netwerk op welke frequentieband zit, de signaalsterkte of er wel of geen beveiliging op zit, het ***MAC-adres*** enz. Vanwege zijn eenvoud was het erg populair, maar aangezien het programma niet onderhouden wordt, werkt het niet (goed) meer op recente

Windows-versies (Vista en later). Een moderne vervanger hiervoor is InSSIDer.

NETWERKANALYZER

Een netwerkanalyzer (ook wel «netwerkmonitor» of «spy» genoemd) is een deelnemer op het netwerk die alle verzonden netwerkverkeer kan ontvangen, analyseren en presenteren in een eenvoudig begrijpbare vorm. Het is meestal een speciaal geschreven softwarepakket dat in combinatie met een netwerkkaart werkt. Soms is het een standaard netwerkkaart, soms is het ook een speciaal voor de analyzer ontworpen netwerkkaart. Dit omdat de analyzer het te analyseren netwerk immers niet mag beïnvloeden. Met het softwarepakket kunnen alle netwerkberichten worden bekeken op inhoud, eventueel gefilterd op tijdstip van transmissie, verzender, ontvanger, commando, een patroon in de data enzovoort.

Men kan dan ook zien welke data door de applicatie aangeboden of verzonden zijn en op welke momenten dat gebeurd is. Dat is zeer nuttig om programmeerfouten uit het applicatieprogramma te halen. Ook kan de netwerkanalyzer worden gebruikt om te bepalen wie de bron is van mogelijke fouten; in gedistribueerde systemen is het immers goed mogelijk dat lokaal een foutmelding gegenereerd wordt door een gebeurtenis op het netwerk bij een deelnemer 300 meter verderop. Met sommige analyzers is het ook mogelijk om de signaalkwaliteit te meten; dat zijn over het algemeen wel de duurdere analyzers.

NETWERKDIODE

Methode om netwerkberichten maar in één richting door te laten. Dit naar analogie met een gewone diode, die stroom maar in één richting doorlaat en in de andere richting blokkeert. Afhankelijk van de richting van de netwerkdiode kan voorkomen worden dat toegang tot een te beveiligen netwerk wordt verkregen, óf dat netwerkberichten naar buiten worden gestuurd.

De “diode” wordt elektrisch gerealiseerd, bijvoorbeeld door van een (normaliter bidirectionele) glasvezelverbinding één glasvezel weg te halen. Het is dus ook fysiek niet mogelijk om netwerkberichten te kunnen versturen tegen de beveiliging in; zelfs malware kan dit niet wijzigen.

Het gebruik van een netwerkdiode brengt wel met zich mee dat zeer veel netwerkprotocollen niet gebruikt kunnen worden, omdat die voor hun interne werking vertrouwen op de mogelijkheid tot bidirectionele communicatie. Met extra hardware en software (zogenaamde “proxy servers”) is dit overigens wel op te lossen.

NETWERKMONITOR

Zie: ***netwerkanalyzer***.

O

OPEN SAFETY

Uitbreiding op het Powerlink protocol voor gebruik in veiligheidstoepassingen. Het heeft echter niets te maken met cybersecurity.

P

PATCH, PATCHEN

Vervangen van een computerprogramma of een deel van een softwarepakket door een nieuwere versie waarin programmeerfouten en/of veiligheidslekken zijn opgelost. Een ander woord dat hier ook wel voor wordt gebruikt is: hotfix.

Meestal bestaat een patch uit een of meerdere nieuwe bestanden, die over de ‘oude’ heen geschreven moeten worden. In Windows kan dit alleen als het te overschrijven bestand niet in gebruik is. Als dat wel zo is, dan wordt het nieuwe bestand tijdelijk ergens anders neer-

gezet, zodat het na een herstart van Windows over het oude heen geschreven kan worden.

De herstart is uiteraard lastig, aangezien de applicatiesoftware dan ook tijdelijk niet (meer) werkt. Dit is de reden dat bij veel bedrijven de installatie van patches pas wordt gedaan op een moment dat het goed uitkomt, bijvoorbeeld tijdens een jaarlijkse stop. De consequentie is dan wel dat men gedurende het hele jaar onnodig kwetsbaar blijft voor bekende cybersecurityproblemen.

Sommige bedrijven (bv. Microsoft) hebben een maandelijkse cyclus, waarbij steeds op een vaste dag patches worden uitgegeven (bv. de tweede dinsdag van de maand bij Microsoft). Dit zorgt ervoor dat systeembeheerders beter hun werk kunnen inplannen, in vergelijking met de methode waarop patches op willekeurige tijdstippen worden uitgegeven.

PENETRATIETEST, PENTEST

Werkwijze waarmee beveiligingsbedrijven proberen toegang te krijgen tot het interne netwerk van een bedrijf. Dit kan op allerlei manieren gebeuren: bijvoorbeeld via Internet, maar ook fysieke toegang tot computers en servers. Op deze manier wordt duidelijk waar de zwakke plekken in de beveiliging van een bedrijf zitten, die eventueel door hackers misbruikt zouden kunnen worden voor datadiefstal, sabotage, etc.

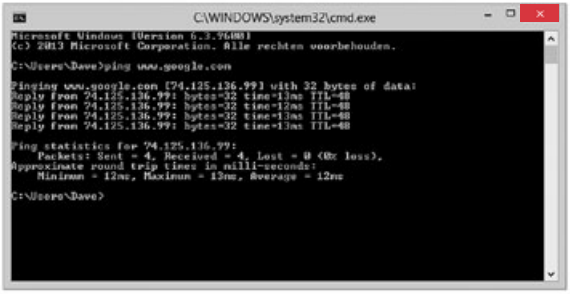
Een penetratietest is bij actieve industriële besturingen af te raden. In de eerste plaats kan de test tot gevolg hebben dat besturingen stoppen met functioneren, vanwege de ongebruikelijke hoeveelheden netwerkberichten en hun specifieke inhoud. Verder kan de gewenste informatie eenvoudiger, sneller en completer verkregen worden door het via een toetsenbord-commando gewoon op te vragen. Bijvoorbeeld, om een MAC- of IP-adres van een (Windows) PC te weten te komen, met welke andere apparaten het communiceert of welke TCP/IP poorten open staan of welke diensten geacti-

veerd zijn volstaan de commando's "ipconfig", "arp" en "netstat".

PING

Oorspronkelijk was 'ping' een eenvoudig Unix-programma (ook beschikbaar op Windows) waarmee men een TCP/IP netwerkbericht naar iemand kon sturen, om te zien of er antwoord terug kwam. Hiermee kan dan eenvoudig gecontroleerd worden of de bekabeling correct is aangelegd, alle software werkt en het andere systeem in de lucht is. Ping is hét gereedschap om dit snel te controleren; als ping aangeeft dat geen contact met het gewenste systeem mogelijk is, dan is het beter om eerst het netwerk in orde te maken en verder geen tijd aan de eigen applicatie te besteden.

Met 'ping' kan eenvoudig vastgesteld worden of een bepaald systeem "up-and-running" is. ▶



Hackers gebruiken vaak ping om op afstand te kunnen detecteren of een bepaald systeem op het netwerk of op internet actief is. Dit is de reden dat firewalls ingesteld kunnen worden om niet te reageren op via internet binnenkomende ping-netwerkberichten.

POLITIEVIRUS

Een virus dat zich voordoet alsof het afkomstig is van de politie (of de belastingdienst of een andere overheidsinstantie). Het geeft een melding op het scherm dat de gebruiker zich schuldig heeft gemaakt aan een misdrijf (bv. download van films, kinderporno, etc.) en vervolging kan afkopen door het overmaken van een bepaald

bedrag naar een (buitenlandse) rekening. Tot die tijd wordt de PC voor normaal gebruik geblokkeerd.

Een variant hierop is het Buma/Stemra (NL) of SABAM (B) virus, dat de gebruiker ervan beschuldigt auteursrechtelijk beschermd materiaal te bezitten. Politievirussen zijn per land anders, zodat het slachtoffer altijd bekende instanties ziet. *Zie ook* ***ransomware***

PORT SCAN

Techniek om te controleren welke applicaties op een systeem benaderd kunnen worden via TCP/IP. Binnen TCP/IP krijgt elke applicatie een (vaste) eigen "poort" waarop het van buiten benaderd kan worden. Bijvoorbeeld, een webserver zal poort 80 gebruiken. Een port scan stuurt een bericht naar alle mogelijke (1..65536) poorten; als daarop een applicatie actief is komt een ander antwoord terug dan wanneer er géén applicatie actief is. Zo kan eenvoudig uitgezocht worden welke applicaties op een apparaat actief zijn.

R

RAM SCRAPER

Malware die het (RAM) geheugen van een processor nazoekt op interessante informatie, zoals wachtwoorden. Alle software bewaart immers gegevens in het RAM-geheugen. Een RAM scraper kan dan zelfs bij gegevens van goed beveiligde software komen. Het uitzetten van de elektronica voor korte tijd helpt ook niet, omdat RAM-geheugen niet meteen gewist wordt.

RANSOMWARE

Malware die de normale werking van een apparaat (meestal een PC) voorkomt of toegang tot alle documenten blokkeert, totdat het slachtoffer een bepaald bedrag heeft overgemaakt. *Zie ook:* ***politievirus***.

RAT

Remote Access Trojan

Benaming voor een categorie ***Trojaanse paarden*** die bedoeld zijn om toegang tot een systeem van buitenaf mogelijk te maken, meestal met het doel om (persoonlijke of zakelijke) informatie te stelen.

RATE LIMITING

Eigenschap van een switch die het mogelijk maakt de netwerkbelasting die via een bepaalde poort wordt ontvangen, onder een (instelbare) grens te houden. Hiermee kan overbelasting van het netwerk voorkomen worden. Dit kan ook nuttig zijn om een broadcast storm of ***babbling idiot*** in bedwang te houden of software die (opzettelijk of onopzettelijk) ongebruikelijk veel netwerkverkeer genereert, zoals in een ***DoS-aanval***.

RED TEAM

Zie: ***blue team***

ROGUE ACCESS POINT

Een access point dat niet onder beheer is van de IT-afdeling, met als doel het uitvoeren van een "Man In The Middle" aanval.

ROOTKIT

Malware die zich in het operating system (de "kernel") verstopt, waardoor ze geheel onzichtbaar is voor alle applicaties en zelfs voor veel ***virusscanners***. Bijvoorbeeld, een rootkit kan alle I/O naar bestanden monitoren en op een leesopdracht andere data teruggeven dan er werkelijk in het bestand staat. De aanwezigheid van de malware in de kernel maakt dat deze toegang heeft tot alle systeemdelen. Het verwijderen van een rootkit moet met zorg gebeuren om de stabiliteit van het systeem niet in gevaar te brengen. Soms is verwijdering alleen mogelijk door het gehele systeem opnieuw te installeren.

RUBBER DUCKY

Generieke naam voor USB-apparaten die er uit zien als memory-sticks, maar het niet zijn. Indien voorzien van een CPU kan een toetsenbord gesimuleerd worden, zodat de besturing van een apparaat kan worden overgenomen. Ook kunnen toetsaanslagen worden gekopieerd, screendumps worden gemaakt, bestanden worden gekopieerd, etc.

S

SANDBOX

Afgeschermde omgeving voor computerprogramma's waarbij deze geen toegang krijgen tot alle delen van het systeem, bijvoorbeeld het geheugen, de harde schijf, het netwerk, het scherm, systeeminstellingen etc. Indien dit toch gewenst is, kan de sandbox dit onder eigen controle uitvoeren. Dit levert een omgeving op om niet-vertrouwde applicaties in uit te voeren, aangezien die dan geen wijzigingen aan het systeem kunnen uitvoeren en dus ook geen software kunnen wijzigen of installeren (wat malware nodig heeft om zichzelf te installeren).

Sandboxen zijn een effectieve techniek om malware tegen te houden; malware auteurs doen daarom hun best om hun malware "uit de sandbox te laten breken". Veel virusdetectors werken ook met sandboxen om te monitoren wat een virus precies wil wijzigen aan een systeem; virussen willen daarom soms detecteren dat ze in een sandbox uitgevoerd worden en doen dan verder niets zodat ze niet gedetecteerd worden.

SCADA

Supervisory Control And Data Acquisition

In de wereld van cybersecurity en door hackers gebruikte verzamelnaam voor "industriële systemen". Dit is zo ontstaan omdat de eerste industriële producten waarvoor hackers interesse kregen PC-gebaseerde SCADA-softwarepakketten waren. Later ging men zich ook richten op PLC's, frequentieomvormers, embedded bestu-

ringen en andere industriële apparatuur, maar de term SCADA is hiervoor in gebruik gebleven.

SCAREWARE

Ogenschijnlijk normale software die zich vaak als ***virusscanner*** voordoet. Aan de gebruiker worden valse meldingen gegeven over de aanwezigheid van malware op het systeem, in de hoop de gebruiker bang te maken ("to scare") en dan te verleiden het "product" te kopen. Na betaling wordt dan de melding verwijderd.

SCHOUDERSURFEN

Over iemands schouder meekijken tijdens de invoer van pincodes en/of wachtwoorden.

SECURITY BY OBSCURITY

Methode om de veiligheid van een apparaat of systeem te garanderen door zo min mogelijk documentatie en informatie erover te verstrekken. Het achterliggende idee is dan dat een potentiële hacker er dan (extra) veel moeite in moet steken om achter de gewenste informatie te komen. Op zich is dit waar, maar het blijkt geen effectieve drempel te zijn. In de praktijk blijkt dat security by obscurity niet werkt tegen vastberaden hackers. Een extra nadeel is dat legale gebruikers ook geen informatie krijgen over hun systeem en dus ook niet weten hoe het te beveiligen en waar de sterke en zwakke punten liggen.

SHA

Secure Hash Algorithm

Een cryptografisch algoritme dat een digitale vingerafdruk berekent van een hoeveelheid elektronische data. Deze vingerafdruk (genaamd "***hash***") is uniek voor die data. Elke wijziging aan die data, hoe klein ook, leidt tot een geheel andere hash. Het is dus géén vorm van encryptie. Een hash heeft een bepaalde lengte in bits, bijvoorbeeld 256. Hoe groter het aantal bits, des te veiliger is de berekende hash. Het werken met hashes is nuttig om vast te stellen of aangeleverde data niet gewijzigd is. Bijvoorbeeld, een leverancier van software kan

hierover een hash uitrekenen en op zijn website publiceren. Iedereen die de software wil controleren kan de hash opnieuw uitrekenen; is deze gelijk aan wat op de website staat dan kan aangenomen worden dat de software niet gewijzigd is. Dezelfde manier van werken kan ook gebruikt worden om te bepalen of een elektronisch document gewijzigd is en of data in archieven niet gewijzigd is. Tenslotte kan een hash gebruikt worden voor het berekenen van een digitale handtekening.

Er zijn diverse varianten van SHA: 0, 1, 2 en 3. SHA-0 bevatte een ontwerpfout en is nauwelijks gebruikt. SHA-1 wordt niet langer als veilig beschouwd. SHA-2 is nog wel veilig (stand: 2014), maar voor de zekerheid is opvolger SHA-3 al wel ontwikkeld. Van SHA-2 bestaan nog diverse varianten, afhankelijk van de lengte van de sleutel met 224, 256, 384 of 512 bits. Naast SHA zijn er nog meer algoritmes, zoals MD5.

SIEM

Security Information and Event Management

Software-applicatie die real-time alle (cyber)security gerelateerde gebeurtenissen in het netwerk verzamelt (en opslaat), kan analyseren en presenteren.

SMARTLISTING

Vorm van een ***blacklisting***, waar software / gebruikers automatisch in geplaatst kunnen worden als een ***intrusion detection system*** aangeeft dat dit nodig is.

SMURFING

Een aanvalstechniek op een netwerk waarbij een netwerkbericht wordt opgesteld met een vervalst afzenderadres, waarna dit (per broadcast) naar alle systemen op een netwerk wordt gestuurd. Deze reageren hierop en sturen hun antwoord allemaal naar het systeem met (valse) afzenderadres, welke daarop overweldigd wordt met inkomend netwerkverkeer.

SNMP

Simple Network Management Protocol.

Een de facto standaard voor een netwerkprotocol dat speciaal ontwikkeld is voor beheer van alle op een netwerk aangesloten apparatuur. Alhoewel SNMP ontstaan is in de zakelijke IT zien we het, dankzij industrieel Ethernet, ook in de industriële netwerkwereld ongewijzigd terugkomen.

Een apparaat moet zijn informatie op een gestandaardiseerde manier aanbieden, zodat dit door elke SNMP implementatie opgehaald kan worden. Welke informatie dit is, is vastgelegd in een zgn. "MIB" – Management Information Base, welke deels vastligt, maar ook nog vrijheden voor de leverancier toelaat. In tegenstelling tot wat de naam suggereert is SNMP niet echt "simpel" meer, omdat het door de jaren heen geëvolueerd is tot wat het nu is.

Een probleem met SNMP is dat velen nog de (oudste) versie 1.0 gebruiken, die geen goede beveiliging tegen hackers biedt. Versie 3.0 biedt die wel.

SPEAR FISHING / PHISHING

Het sturen van een officieel uitziende e-mail met een link of een besmette attachment erbij, met een zodanig lokkende tekst dat de gebruiker verleid wordt op de link te klikken of de attachment te openen, waardoor automatisch een besmetting plaatsvindt. Hierbij wordt vaak gebruik gemaakt van (ogenschijnlijk) PDF-documenten, die echter ook de malware bevatten.

Ook kunnen e-mails verstuurd worden met persoonlijke informatie er in en afkomstig van collega's of familie. Deze informatie kan vaak eenvoudig via social media (Facebook, LinkedIn, etc.) gevonden worden. Het geeft de e-mail een schijn van betrouwbaarheid, waardoor de kans dat de lezer erop reageert groter wordt.

Een derde vorm van spear fishing is het sturen van een e-mail waarin de lezer wordt meegedeeld dat door een extern probleem alle wachtwoorden gereset zijn en of de lezer deze ter verificatie opnieuw wil invoeren om te voorkomen dat zijn account permanent geblokkeerd wordt.

SPY

Zie: ***netwerkanalyzer****.*

SSID

Service Set ID

De 'naam' van een draadloos (IEEE 802.11 / WiFi) netwerk, welke regelmatig wordt verzonden zodat een in de buurt aanwezige gebruiker kan zien welke draadloze netwerken ter beschikking staan.

Om potentiële hackers geen direct bruikbare informatie te geven wordt afgeraden om de naam van het bedrijf, divisie of afdeling op te nemen in de SSID, maar enkel een voor derden nietszeggende tekst.

Vaak wordt als beveiligingsmaatregel genoemd dat een draadloos netwerk niet regelmatig zijn SSID rondstuurt, met het idee dat het dan ook niet te ontdekken is. Dat is natuurlijk niet zo, elk draadloos verzonden netwerkbericht kan opgevangen worden ook al is de SSID niet bekend.

STATEFUL FIREWALL

Variant van een gewone ***firewall***. Normaliter kijkt een (stateless) firewall alleen maar naar de inhoud van ontvangen netwerkberichten en neemt op basis van deze inhoud de beslissing wat er verder met dat netwerkbericht gedaan moet worden: blokkeren of doorsturen. Een stateful firewall kijkt ook naar de samenhang tussen netwerkberichten en kan dus op andere criteria besluiten nemen. Bijvoorbeeld: komt de hoeveelheid data in een antwoord overeen met de eerder aangevraagde hoeveelheid data? Past dit netwerkbericht wel in de con-

text van eerder afgehandelde netwerkberichten? Komen er op één vraag misschien meerdere antwoorden terug? Wie neemt het initiatief? Etc.

Een stateful firewall moet dus wel kennis hebben van gebruikte protocollen. Dit is voor industriële protocollen nog vrij ongebruikelijk; voor de standaard protocollen zoals TCP/IP is het gemeengoed.

STEALTH MODE

Manier van werken van een firewall of WiFi access point, waarbij deze geheel of gedeeltelijk onzichtbaar is op een netwerk.

Wanneer we bij een firewall spreken over Stealth mode, dan bedoelen we hiermee een manier van werken waarbij de firewall (eventueel ook achteraf) volledig transparant in een bestaand netwerk wordt geïntegreerd. De firewall neemt daarbij automatisch de MAC- en IP-adressen van de te beveiligen systemen over, zodat er geen extra adressen voor het management van de firewall nodig zijn. Ook hoeven er geen andere aanpassingen in de netwerkconfiguratie te worden uitgevoerd.

Wanneer we bij een Access point in IEEE 802.11 / WiFi-netwerk over Stealth mode spreken dan bedoelen we hiermee een manier van werken waarbij niet meer regelmatig de netwerknaam (***SSID***) per broadcast wordt verstuurd. Normaliter wordt dit juist gedaan om de aanwezigheid van een netwerk bekend te maken aan bezoekers, bijvoorbeeld in een openbare gelegenheid. Maar dit houdt ook in dat hackers eenvoudig te weten kunnen komen welke WiFi-netwerken actief zijn, eenvoudigweg door enkele seconden te luisteren. In toepassingen waarbij een WiFi-netwerk altijd vaste gebruikers heeft, is het niet noodzakelijk om het SSID regelmatig rond te sturen. Dit maakt het netwerk 'onzichtbaar' op een gewone PC, tablet of mobiele telefoon.

Werken in stealth mode wordt vaak als beveiligingsmaatregel voor WiFi-netwerken genoemd, maar het is voor een vastberaden hacker slechts een kleine drempel.

STUXNET

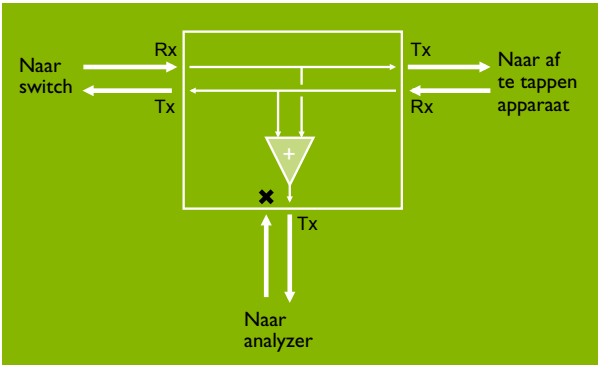
Zie: ***hoofdstuk 5***.

T

TAP

Apparaatje waarmee het mogelijk is om Ethernet-berichten "af te tappen" en een kopie door te sturen naar een extra aan te sluiten apparaat, meestal een ***netwerkanalyzer*** of een ***intrusion detection system***.

Er bestaan een aantal soorten taps, de meest gangbare is een "aggregrating tap" die beide richtingen netwerkverkeer combineert en als één geheel aanbiedt aan de netwerkanalyzer, die daarom ook kan volstaan met één netwerkaansluiting.



▲ Principeschema van een 100 Mbit/s Ethernet aggregating tap.

Taps zijn, vanwege hun kleine verkochte aantallen, vrij kostbaar in aanschaf (reken op ca. 1000 Euro). Let er ook op dat een tap als actieve deelnemer 'in' het pad tussen twee apparaten zit en uitval van de tap dus ook leidt tot een communicatiestoring. Sommige merken taps hebben daarom ook een redundante voedingsaansluiting.

TELEGRAM

Veelgebruikte benaming voor een netwerkbericht.

TROJAN, TROJAANS PAARD

Vorm van malware die zich via een slinkse weg op een systeem laat installeren, bijvoorbeeld door zich voor te doen als nuttige software en daarom door de gebruiker op zijn systeem wordt geïnstalleerd. Eenmaal actief, heeft het toegang tot het systeem en kan daar schade aanrichten en/of toegang tot data krijgen.

Het verschil met een worm is dat deze laatste zichzelf verder gaat verspreiden; een Trojan wordt vaak per e-mail aangeleverd of verstopt in andere programmatuur waarna het aanstaande slachtoffer verleid moet worden dit te installeren. *Zie ook:* ***RAT***.

U

USB CONDOOM

Een speciale verloopstekker of -kabel om USB-apparatuur aan te sluiten, maar waarin de beide netwerkaders onderbroken zijn. Er is dan geen communicatie met het USB-apparaat mogelijk, zodat ook geen malware op het apparaat geïnstalleerd kan worden of data er afgehaald kan worden. Het biedt dus een wederzijdse bescherming. De beide voedingsaders zijn wel doorgeschakeld, zodat opladen wel mogelijk is. De eigenaar van het USB-apparaat kan dus met vertrouwen zijn apparatuur opladen op locaties waar wel een USB-aansluiting is, maar onduidelijk is wat er precies 'achter' zit (bv. in hotels, vliegvelden, onbekende PC's, etc.). *Zie ook:* ***juice jacking***.

V

VIRUS

Meest bekende variant van ***malware***, die zich ongezien en autonoom op een systeem installeert. Het verschil

met een ***Trojan*** is dat hier de malware verstopt zit in nuttig lijkende software. Het verschil met een ***worm*** is dat deze laatste zich zelfstandig verspreidt. Daarentegen zit een virus vaak verstopt in een ander programma en kan dus pas geactiveerd worden zodra dat programma opgestart wordt.

Voor de gemiddelde gebruiker is er geen verschil tussen Trojans, virussen en wormen; een ***virusscanner*** zal ze allemaal pogen te detecteren en te verwijderen.

VIRUSSCANNER

Programma dat poogt te detecteren of een virus, trojan, worm of een andere vorm van malware wil binnendringen op een systeem. Dit wordt gedaan door alle communicatiepaden van dat systeem te bewaken: USB, netwerk (bekabeld en draadloos), floppies, etc. Ook kunnen bestanden op het filesysteem worden gecontroleerd, de harde schijf zelf, het eigen geheugen en andere plekken waar malware zichzelf kan nestelen, evenals de opstartcommando's.

Malware wordt gedetecteerd aan de hand van de datapatronen in de bestanden van de malware zelf, de zogenaamde "signatures". De virusscanner-leverancier maakt een database met daarin alle bekende signatures en verspreidt deze database weer onder zijn klanten. Dit kan meerdere malen per uur gebeuren. Een signature database die niet geactualiseerd blijft, verliest heel snel zijn waarde, aangezien de modernste malware dan niet meer door de virusscanner gedetecteerd kan worden.

W

WAR CHALKING

Het met krijt op de muur van een gebouw schrijven welk draadloos netwerk bereikbaar is, welke naam het heeft en hoe het staat met de beveiliging van dit netwerk. Aan de hand van deze informatie kan een hacker dan eenvou-

dig zien hoe van dit draadloze netwerk gebruik gemaakt kan worden. De kreet war chalking is uitgevonden door een Britse journalist. Het hele verhaal is waarschijnlijk verzonnen, maar is wel de hele wereld rondgegaan en wordt nog regelmatig aangehaald als voorbeeld van de kwetsbaarheid van draadloze netwerken.

WAR DRIVING

Het met een auto en een WiFi-ontvanger rondrijden met als doel zoveel mogelijk WiFi-netwerken te vinden. Het is gebruikelijk om zoveel mogelijk informatie over de gevonden WiFi-netwerken (leverancier, type, ***MAC-adres***, snelheid, wel of geen wachtwoord, etc.) in een database op te slaan. Indien deze informatie ook gekoppeld wordt aan een GPS-coördinaat kunnen websites automatisch kaarten maken.

WATERING HOLE ATTACK

Het besmetten met malware van websites die door de beoogde slachtoffers veelvuldig bezocht worden. Welke website(s) dit moeten zijn, kan uit een analyse van netwerkverkeer blijken. Na installatie van de malware op de website zal infectie automatisch volgen. Deze aanvalsmethode is specifiek bedoeld voor bepaalde personen, bedrijven of instanties.

WEP

Wired Equivalent Privacy

Encryptiealgoritme dat in de eerste versies van WiFi beschikbaar was, maar door diverse wiskundige zwakheden in het algoritme erg eenvoudig te kraken is. Het wereldrecord WEP-kraken staat nu op minder dan één seconde rekentijd. Het gebruik van WEP wordt daarom zeer sterk afgeraden. De opvolger van WEP is ***WPA2*** met ***AES*** als encryptiestandaard.

WHITELISTING

Methode waarmee toegang wordt gegeven tot een systeem, machine, ruimte, softwarepakket, netwerkadres, protocol, etc. aan iedereen die op de “witte lijst” staat.

Het altijd genoemde nadeel van whitelisting is dat de lijst in snel wijzigende omgevingen altijd verouderd is. Dat is in kantooromgevingen ook wel zo, maar in industriele systemen is het anders: hier wordt vaak jarenlang dezelfde software gebruikt met dezelfde apparatuur en een kleine groep gebruikers. De veel stabielere omgeving maakt whitelisting daarom eenvoudiger in gebruik.

De tegenovergestelde methode van whitelisting is ***blacklisting***.

WIRESHARK

Naam van een open-source Ethernet ***netwerkanalyzerpakket***, dat o.a. op PC's, MAC's en Linux-systemen kan draaien. Het is de opvolger van het oudere Ethereal, waarvan de ontwikkeling gestopt is. Wireshark biedt ondersteuning voor enkele honderden protocollen, waaronder ook inbegrepen enkele industrieel Ethernet varianten. Website: www.wireshark.org.

Het gebruik van Wireshark (of elke andere netwerkanalyzer) maakt dat naar de inhoud van netwerkberichten gekeken kan worden. Let er op dat informatie ook bij de verkeerde personen terecht kan komen (zoals beurskoersgevoelige informatie). Het gebruik van netwerkanalyzers is in sommige bedrijven daarom ook verboden. Systeembeheerders kunnen met speciale programma's het gebruik van netwerkanalyzers detecteren.

WORM

Computerprogramma dat zich zelfstandig van de ene naar de andere computer kan verspreiden (in tegenstelling tot een ***virus*** is hiervoor geen applicatiesoftware nodig). Een worm die jarenlang actief geweest is en veel schade heeft aangericht is ***Conficker***.

WPA2

WiFi Protected Access 2

Actuele beveiligingstechniek voor draadloos Ethernet (WiFi), als opvolger van ***WEP***. Dankzij gebruik van een

zeer sterk encryptiealgoritme (***AES***) is het nog steeds niet gelukt om de encryptie te kraken zolang maar gebruik wordt gemaakt van een sterk wachtwoord. Korte wachtwoorden zijn (uiteraard) nog gewoon met een ***brute force*** aanval te raden.

Z

ZERO DAY

Aanval op een systeem die gebruik maakt van een nog ongepubliceerd lek in software. Zodra het lek bekend is ("dag 1") bij de ontwikkelaar van die software maar het lek nog niet gedicht is, kan een zero-day aanval succesvol zijn. Hackers pogen steeds sneller bekende lekken te misbruiken vóórdat de leverancier er op kan reageren; door ***defense in depth*** maatregelen te nemen kan men toch nog tegen een zero day beschermd zijn.

Wordt het lek nooit gedicht, dan wordt ook wel van een ***forever day*** aanval gesproken.

ZOMBIE

Andere benaming voor een ***bot***.

Cyber Compendium
Rob Hulsebos

Na de ontdekking van het Stuxnet-virus steeg de belangstelling voor de beveiliging van industriële besturingssystemen, zowel vanuit de industrie en de overheid als vanuit de hackers. Alles waar software in zit én een netwerkverbinding heeft, is namelijk in principe kwetsbaar.

Alhoewel 'Hollywood' het doet voorkomen alsof hackers met een paar toetsaanslagen in elk systeem kunnen binnendringen, is dit geen dagelijkse praktijk. Hackers (en criminelen!) maken liever misbruik van onze onwetendheid en onkunde op dit gebied.

Deze publicatie is bedoeld als inleiding tot de zeer uitgebreide en dynamische wereld van de (industriële) cybersecurity. Geschreven vanuit de praktijk en herkenbaar voor iedereen die werkzaam is in de industrie. Zodat aandacht voor cybersecurity een dagelijks onderdeel wordt van elk project, in elk systeem, in elk bedrijf.

www.phoenixcontact.nl
www.phoenixcontact.be

PHOENIX CONTACT
INSPIRING INNOVATIONS