

Een common practice op het gebied van beveiligingstools

Inhoudsopgave

1.	Inleiding	3
2.	Trends.....	4
3.	Bedreigingen en oplossingen	5
3.1.	Algemeen	5
3.2.	Controle over netwerk.....	6
3.2.1.	Bescherming aan de poort.....	6
3.2.2.	Specifiek filteren	7
3.2.3.	Bescherming bij gebruikers	7
3.2.4.	Identificeren van bedreigingen.....	8
3.2.5.	Totaaloplossingen	8
3.2.6.	Draadloze netwerken.....	9
3.3.	Controle over data en applicaties	9
3.3.1.	Bescherming van data(opslag).....	9
3.3.2.	Bescherming van databases	10
3.3.3.	Bescherming van applicaties.....	11
3.4.	Raakvlakken.....	12
3.4.1.	Identity management	12
3.4.2.	Processen en gedrag	12
3.4.3.	Business continuity	13
4.	Rol SURFnet	15

1. Inleiding

Dit rapport is onderdeel van het SURFworks-project 'Verkenning Beveiligingstooling'. Het doel van dit project is het ontwikkelen van een common practice op het gebied van beveiligingstools en het verkrijgen van inzicht in de door de op SURFnet aangesloten instellingen gewenste rol van SURFnet. Dit rapport geeft een invulling aan beide aspecten van het doel. Met dit project wordt een belangrijke randvoorwaarde geschapen voor een samenwerking met SURFdiensten op het gebied van informatiebeveiliging¹.

In de eerste fase van het project zijn interviews met aangesloten instellingen gehouden om de wensen en behoeften op het gebied van informatiebeveiliging bij de instellingen te inventariseren. Vervolgens is er onderzoeksmateriaal verzameld over de huidige stand van zaken ten aanzien van informatiebeveiliging, cybercrime en de markt van beveiligingstools. Deze twee bronnen vormden de basis bij het schrijven van dit rapport.

Het rapport bestaat voornamelijk uit het beschrijven van de belangrijkste trends en producten om zo tot een *common practice* te komen van functionaliteit op het terrein van informatiebeveiliging. Daarna wordt het rapport afgesloten door in te gaan op de rol van SURFnet binnen beveiliging en wordt geschetst wat er verder nodig is voor een samenwerking met SURFdiensten.

Als bronmateriaal heeft dit rapport voor een groot deel gebruik gemaakt van onderzoeksrapporten van Gartner, een internationaal onderzoeksbureau dat zich voornamelijk richt op ICT-ontwikkelingen. Het internationale karakter van dit materiaal betekent wel dat de nadruk ligt op leveranciers van enige omvang, die doorgaans internationaal opereren. Hierdoor kan het zijn dat er lokale leveranciers ontbreken, die binnen het hoger onderwijs en onderzoek in Nederland toch een rol van betekenis spelen. Om deze reden is het in dit rapport nog niet mogelijk om een standaardpakket aan tools aan te bevelen. De focus van dit rapport ligt hierdoor op het beschrijven van functionaliteit en niet zozeer op het beschrijven van leveranciers. Voor dergelijke specifieke informatie is het altijd mogelijk om contact op te nemen met SURFnet.

Evenals in het rapport 'Beveiliging bij de aangesloten instellingen' wordt ook hier de volgende definitie voor informatiebeveiliging gebruikt:

Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.²

Er wordt geen onderscheid gemaakt tussen databeveiliging en systeembeveiliging; beide worden als onderdeel van informatiebeveiliging beschouwd.

¹ In het jaarplan SURFworks 2009 was het oorspronkelijke doel van dit project om in samenwerking met SURFdiensten tot een standaardpakket aan beveiligingstools te komen. Deze insteek is in de loop van het project gewijzigd: het is in deze fase nog niet mogelijk om een standaardpakket aan te bevelen. SURFnet en SURFdiensten zijn voornemens dit in de loop van 2010 te realiseren.

² <http://nl.wikipedia.org/wiki/Informatiebeveiliging>

2. Trends

Instellingen genereren steeds meer data en gebruiken ICT in steeds meer processen. Hierdoor is de afhankelijkheid van ICT zo groot geworden, dat het noodzakelijk is om een overzicht te hebben van de belangrijkste maatregelen die genomen moeten worden om zich te kunnen wapenen tegen de gevaren die op dit moment spelen op het gebied van informatiebeveiliging. Dit strekt zich uit over meerdere niveaus. Het is niet alleen van belang om een veilige omgeving op een computer te bieden, ook het netwerk zelf dient beveiligd te worden, waarbij de omgang met mobiele devices als laptops, smartphones en USB sticks tot nieuwe risico's heeft geleid. Georganiseerde aanvallen op draadloze netwerken en het lekken van gegevens vanaf mobiele devices zijn al regelmatig in het nieuws geweest. Het kwijtraken van een USB-stick of een smartphone met gevoelige informatie kan iedereen overkomen, belangrijk is dan of en hoe dergelijke apparaten beveiligd zijn. Het goed beheren van rollen en rechten van (ex-) gebruikers is natuurlijk essentieel, maar doorslaggevend is hoe die gebruikers omgaan met hun rechten en de gedragsregels. Een door de gehele organisatie gedragen informatiebeveiligingsbeleid is gezien het bovenstaande onontbeerlijk. In het hoger onderwijs zien we dit besef steeds meer terug door de centrale positie die informatiebeveiliging inneemt binnen de organisatie.

Inbreuk op informatieveiligheid heeft zich de afgelopen jaren bovendien steeds meer verfijnd. Waar het voorheen meer uit hobbyisme werd gedaan en waar aanvallen willekeurig waren of een brede aanpak hadden, om op zo veel mogelijk plekken schade aan te richten, laten trends nu zien dat aanvallen steeds professioneler worden uitgevoerd met eerder financiële motieven dan ideologische of politieke motieven. Hierdoor zijn aanvallen steeds vaker gericht op specifieke doelen zoals het stelen van identiteiten of creditcardinformatie. Ook zijn er steeds meer verschillende typen van aanval: waar voorheen vooral gezocht werd naar niet voldoende beveiligde pc's, zijn nu ook websites en gebruikers het doelwit van cybercrime. Denk hierbij aan phishing; het verleiden van gebruikers tot het geven van persoonlijke informatie zoals wachtwoorden. De georganiseerde misdaad houdt zich hier al geruime tijd strategisch mee bezig.

Wereldwijd wordt men zich meer en meer bewust van het belang van een gecoördineerde aanpak van informatiebeveiliging. Zo hebben de Verenigde Staten een Cybersecurity Coordinator aangesteld om landelijk informatiebeveiliging te kunnen coördineren en doet men in Engeland onderzoek naar de status van cybersecurity bij de overheid. Ook in Nederland wordt er steeds meer aandacht besteed aan informatiebeveiliging, getuige de campagne 'Veilig Internetten heb je zelf in de hand' (zie <http://www.veiliginternetten.nl>). Binnen de SURFnet doelgroep worden sinds enkele jaren awareness campagnes georganiseerd, met als recent voorbeeld de campagne *CyberSave Yourself (CSY)*.

3. Bedreigingen en oplossingen

3.1. Algemeen

De trends laten zien dat de professionalisering van cybercriminelen en de afhankelijkheid van ICT processen in de organisatie een gedegen en brede aanpak van informatiebeveiliging vragen. In het nu volgende deel wordt ingegaan op de bedreigingen en oplossingen binnen de deelgebieden van informatiebeveiliging. De nadruk ligt daarbij op *controle over het netwerk* en *controle over data en applicaties*, de twee centrale gebieden van informatiebeveiliging. Deze thema's zijn verder uitgewerkt in sub-categorieën die specifieke beveiligingsproducten beschrijven. Vervolgens worden de thema's *identity management*, *processen en gedrag* en *business continuity* behandeld. Vanwege de wat abstractere aard van deze thema's, is hier gekozen voor een meer beschrijvende benadering.

In de categorieën *controle over het netwerk* en *controle over data* worden steeds enkele voorbeeldleveranciers genoemd. Hiermee wil SURFnet per deelgebied een indicatie geven van partijen die in ieder geval een sterke positie innemen. Het is echter geenszins de bedoeling van dit rapport om een advies aan de instellingen uit te brengen over welke leveranciers zij moeten inschakelen, omdat dit kennis van de specifieke situatie bij de instelling vereist.

Bovendien zijn de genoemde voorbeeldleveranciers zoals eerder aangegeven meestal grote, internationale spelers. Het is dan ook zeker niet uit te sluiten dat een lokaal opererende leverancier beter dan deze spelers in kan spelen op specifieke behoeftes binnen het hoger onderwijs en onderzoek. Ook *open source* en *freeware* oplossingen komen minder aan bod. Dit heeft enerzijds te maken met de beschrijving op functioneel niveau, anderzijds laten ze zich moeilijk(er) vergelijken met traditionele leveranciers. Op internet zijn talloze voorbeelden te vinden van open source tools, die op deelgebieden een uitstekende oplossing kunnen bieden. Zie bijvoorbeeld de website <http://www.insecure.org>, waar een *Network Security Toolkit* wordt aangeboden met de meest gangbare open source tools.

Kortom, er bestaat geen kant-en-klaar pakket van maatregelen, waarmee een organisatie zeker weet dat de informatie 100% beveiligd is. Dit hangt te zeer af van de lokale situatie, zoals de grootte en complexiteit van het netwerk maar ook van processen en van het gedrag van de gebruikers. Wel is er een bepaald patroon terug te zien in de te nemen maatregelen. Zo zijn alle maatregelen te verdelen in preventieve, detectieve, repressieve en correctieve maatregelen. Dit vertaalt zich in het beperken van de mogelijkheden van kwaadwillenden, het bijhouden van alle mogelijke gedragingen op het netwerk of rond data en applicaties (zodat analyses achteraf gedaan kunnen worden) en het snel kunnen herstellen van inbreuken en calamiteiten.

3.2. Controle over netwerk

3.2.1. Bescherming aan de poort

Het internet is een groot netwerk van aan elkaar verbonden kleinere netwerken. Op de grens van het eigen netwerk en de rest van de wereld begint het nemen van veiligheidsmaatregelen. De meeste aanvallen of bedreigingen komen van buiten af: een externe persoon of applicatie wil het instellingsnetwerk binnen dringen om gebruik te kunnen maken van interne informatie, iemand wil het instellingsnetwerk afsluiten van de rest van de wereld, etc.

Twee veelgebruikte methoden om illegaal verkeer van buitenaf te blokkeren zijn de inzet van een firewall of een Intrusion Prevention System (IPS; deze oplossingen gaan verder dan Intrusion Detection Systems (IDS) die zich slechts beperken tot het analyseren en detecteren van aanvallen). Een firewall bepaalt traditioneel of de poort waarop verkeer binnen komt open staat voor verkeer van buitenaf en of het protocol, de taal waarin het verkeer wil communiceren, toegestaan is.

Waar een traditionele firewall kijkt naar algemene kenmerken van het verkeer, daar kijkt een IPS juist naar de details. Netwerkverkeer bestaat uit een reeks van pakketjes met velden van informatie, gedefinieerd door het protocol dat gebruikt wordt door het pakketje. Wanneer verdacht verkeer gekenmerkt wordt door bepaalde patronen in die informatievelden, kan een IPS een regel ontwikkelen die ervoor zorgt dat bij dergelijke patronen het verkeer geblokkeerd wordt. Een eenvoudig patroon is bijvoorbeeld het blokkeren van verkeer van een specifieke afzender, complexere patronen bestaan uit combinaties van informatievelden. Een IPS wordt ook gebruikt door leveranciers om typisch verdacht verkeer aan te merken. Wanneer een fout is ontdekt in bijvoorbeeld een besturingssysteem komt er over het algemeen kort erna een patch uit die de fout repareert. Deze patch dient geïnstalleerd te worden op alle systemen om misbruik van de fout te voorkomen. In de tussentijd is het mogelijk voor de leverancier om specifieke kenmerken van verkeer aan te merken dat misbruik maakt van deze fout. Zo kan een IPS dus 'pre-patch' bescherming bieden aan systemen wanneer een leverancier deze kenmerken aanlevert. De bruikbaarheid hiervan is overigens vaak beperkt, wanneer leveranciers slechts in beperkte detail treden over het betreffende patroon.

Overigens hoeft een firewall of een IPS niet perse geplaatst te worden aan de rand van het netwerk. Het kan ook verstandig zijn om specifieke locaties binnen het netwerk extra te beschermen met een eigen speciaal geconfigureerde firewall of IPS. Waar dergelijke locaties steeds vaker gevirtualiseerd worden, geldt dit ook in toenemende mate voor hun firewalls.

De laatste ontwikkelingen op dit gebied wijzen in de richting van een convergentie van bovengenoemde methoden, ook wel Next-Generation Firewalls (NGFW) genoemd. Hoewel de beste firewalls vaak ook een primitieve vorm van IPS bevatten en andersom, bereiken deze zelden het niveau van de individuele producten. Dit is echter het begin van de ontwikkeling van NGFWs waarin elk onderdeel goed presteert. Een dergelijke suite van producten zal bovendien ook andere elementen bevatten zoals het identificeren en al dan niet toelaten van (web)applicaties die zich specifiek gedragen (denk aan instant messaging, peer-to-peer verbindingen of pc remote control).

Leveranciers

Juniper Networks, Cisco Systems, Fortinet, Quarantainenet

3.2.2. Specifiek filteren

Waar Intrusion Prevention Systems zich richten op generieke filtering van verkeer, zijn er ook verschillende producten op de markt die zich specifiek richten op het filteren van de inhoud van het verkeer op bekende bedreigingen of onbekend gedrag.

Secure Web Gateways (SWG) zijn producten die ongewenste software en malware filteren uit door gebruikers geïnitieerd web- of internetverkeer en die bovendien huisregels of groepsregels kunnen afdwingen. Een SWG doet minimaal aan URL-filtering en het detecteren en filteren van kwaadaardige code. De voorlopige SWGs bieden daarnaast enige controle op webapplicatie-niveau (instant messaging, games, kantoorapplicaties, etc.) waarbij ze ook letten op vreemd gedrag van applicaties van binnen het netwerk naar buiten toe. SWGs zijn geëvolueerd uit oudere producten zoals proxy servers, URL-filtering en Web gateway antivirus.

Het internet is tegenwoordig de grootste bron van infecties voor pc's. Hoe meer mensen gebruik maken van online applicaties, blogs en sociale netwerken (Hyves, LinkedIn, etc.), hoe moeilijker het is om controle uit te oefenen over het verkeer dat in en uit het netwerk stroomt. De producten onder de noemer SWGs ontwikkelen zich meer en meer richting volwassen producten die deze controle bieden. Hoewel het wenselijk is om dergelijke controle op verschillende manieren toe te passen afhankelijk van de groepen gebruikers die er bestaan, dienen gebruikers zelf zo weinig mogelijk van het gedrag van SWGs te merken, met name in termen van snelheid en prestatie van de internetverbinding.

Naast controle over webverkeer bestaan er ook producten die controle over e-mailverkeer bieden. Gezien de enorme hoeveelheden spam die tegenwoordig wordt verstuurd, is dit een onmisbare schakel in het beveiligen van het netwerk. Naast anti-spam, zijn antivirus, het filteren van verkeer van binnen naar buiten en versleuteling van e-mailverkeer belangrijke functionaliteiten van beveiligingsoplossingen voor e-mail. De effectiviteit van deze oplossingen wordt steeds meer bepaald door de mate waarin ze de constant veranderende bedreigingen kunnen bijhouden.

Het ligt voor de hand dat in de toekomst verschillende soorten specifieke filters worden samengebracht in een applicatie. Er zijn nu al producten op de markt die dergelijke functionaliteit bieden en de verwachting is dat dit aantal sterk zal toenemen. Dit wordt niet alleen ingegeven door gemak voor klanten en synergievoordeel, maar ook door steeds complexere aanvallen over meerdere soorten verkeer (protocollen).

Essentieel voor het succes van dit soort geavanceerde tools is wel dat het lokale beheer goed ingevoerd is in de bewaking ervan; fouten in de (functioneel complexe) configuratie kunnen zelfs leiden tot grotere schade.

Leveranciers

SWG: Blue Coat Systems, Secure Computing, Aladdin Knowledge Systems

E-mail: Cisco/Ironport, Google/Postini, Symantec, Proofpoint, Roaring Penguin

3.2.3. Bescherming bij gebruikers

Het eigen netwerk begint bij een ingang of verbindingspoort naar andere netwerken en eindigt bij (de pc van) elke gebruiker van het netwerk. Bescherming aan de poort is efficiënt en ligt voor de hand, maar is vaak niet voldoende om gebruikers tegen alles te beschermen (vooral veroorzaakt door een zekere balans tussen de vrijheid die eigen gebruikers wordt gegeven en de striktheid waarmee inkomend en uitgaand

verkeerd wordt gecontroleerd). Daarom wordt er gebruik gemaakt van antivirussoftware of persoonlijke firewalls. Ook zijn er tools beschikbaar waarmee gecontroleerd kan worden of software op de werkplek up-to-date is.

Endpoint Protection Platforms (EPPs) zijn oplossingen waarin verschillende beveiligingsproducten zijn samengebracht in een suite. Het gaat hierbij om minimaal antivirus, anti-spyware, persoonlijke firewalls en host-based intrusion prevention systems (HIPS). EPPs brengen deze producten samen in een overzichtelijk pakket waarin ze op een plek geconfigureerd en gemanaged kunnen worden. Bovendien zorgt deze convergentie voor meer gebruikersgemak omdat een EPP minder capaciteit vraagt van een pc dan de afzonderlijke producten bij elkaar. Naast de genoemde oplossingen ontwikkelen EPPs zich ook door het toevoegen van versleuteling van data(schijven) en het voorkomen van dataverlies. Een belangrijke eigenschap van EPPs is verder dat ze beter zijn toegerust om complexe of onbekende bedreigingen tegen te gaan door bijvoorbeeld softwaremanagement of whitelisting (alleen met toestemming van de eigenaar van een EPP wordt een bepaalde bron vertrouwd). Dit in tegenstelling tot traditionele oplossingen als antivirus die vaak alleen effectief zijn tegen bekende bedreigingen (reactief gedrag).

Leveranciers

McAfee, Symantec, Sophos, Secunia

3.2.4. Identificeren van bedreigingen

Ieder netwerk heeft zijn eigen specifieke kenmerken en zijn eigen context. Hoewel een netwerk veelal goed beschermd kan worden door oplossingen die door de markt worden geboden, zorgen deze specifieke kenmerken ervoor dat er unieke situaties of bedreigingen kunnen ontstaan die niet (standaard) kunnen worden afgedekt door deze oplossingen. Het is daarom belangrijk om te weten welke soort aanvallen het meeste voorkomen en om achteraf te kunnen achterhalen waarom een aanval succesvol was.

Security Information and Event Management (SIEM) oplossingen worden gebruikt om data over beveiligingsgebeurtenissen (real-time) te analyseren zodat bedreigingen gemanaged kunnen worden en om gegevens te verzamelen zodat achteraf analyses gemaakt kunnen worden. Deze analyses kunnen bijvoorbeeld worden gebruikt om te kijken of het netwerkverkeer zich gedraagt zoals verwacht mag worden gegeven de beveiligingsmaatregelen die zijn genomen. Belangrijk voor SIEM oplossingen is dat ze zowel real-time als achteraf data (uit bv. logs) zo kunnen verwerken dat ze overzichtelijke analyses kunnen maken, relaties kunnen leggen tussen verschillende gebeurtenissen, informatie van verschillende bronnen kunnen normaliseren en bovenal dat ze helder en begrijpbaar rapporteren. Wanneer een netwerk gemonitord wordt door een goed toegepaste SIEM, zullen beheerders adequater kunnen reageren op bedreigingen en beveiligingsincidenten.

Leveranciers

RSA, ArcSight, IBM

3.2.5. Totaaloplossingen

Netwerken van kleine instellingen vragen over het algemeen iets anders qua beveiliging dan grote complexe netwerken. Gemotiveerd door het relatief eenvoudige netwerk, financiële beperkingen en eventueel een gebrek aan specialistische kennis, zijn zij eerder op zoek naar totaaloplossingen. Een pakket waarin alle maatregelen om het netwerk te beveiligen samen komen in een overzichtelijk en makkelijk configureerbaar geheel. Dergelijke oplossingen worden Multifunction Firewalls genoemd.

Multifunction Firewalls richten zich specifiek op de kleinere netwerken en zijn niet geschikt voor grote complexe netwerken. Deze totaaloplossingen bieden vaak een firewall als basisproduct waarop allerlei uitbreidingsmogelijkheden zijn. Deze uitbreidingen vallen in drie categorieën: netwerkbeveiliging (firewalls, Intrusion Prevention Systems, Virtual Private Networks (VPNs), etc.), webbeveiliging (URL-filtering, web antivirus, etc.) en e-mailbeveiliging (antispam, e-mail antivirus, etc.). De uitbreidingen zullen zelden het niveau halen van afzonderlijke oplossingen, maar zijn over het algemeen gericht op en goed genoeg voor kleinere netwerken. Bovendien biedt een dergelijke integratie gemak en overzicht voor beheerders met minder specifieke kennis.

Leveranciers

Fortinet, SonicWall, WatchGuard

3.2.6. Draadloze netwerken

Tot op zekere hoogte verschillen draadloze netwerken weinig van normale bedrade netwerken. Alles wat hierboven besproken is, is van toepassing op beide typen netwerken. Het bijzondere aan draadloze netwerken is dat toegang mogelijk wordt gemaakt door radiogolven in plaats van een plug in de muur. Dit maakt dat toegang minder locatiegebonden is en vaak buiten het gebouw mogelijk is. Waar in een bedraad netwerk fysieke beveiliging (iemand moet eerst toegang hebben tot een plug in de muur) de eerste basale verdediging is tegen kwaadwillenden, ontbreekt dit bij draadloze netwerken. Dit zorgt voor een extra dimensie in beveiliging.

Voor draadloze netwerken is het voorkomen van toegang door onbevoegden iets dat extra aandacht verdient. Het komt regelmatig voor dat men onvoorzichtig is bij het configureren van draadloze netwerken, vooral bij kleinere (thuis)netwerken. Vanwege gebrek aan kennis of een onderschatting van de gevaren, zijn dergelijke draadloze netwerken openlijk toegankelijk. Er zijn verschillende manieren om deze risico's te voorkomen, met name door enkele (eenvoudige) configuratieaanpassingen. Voor grotere (publieke) draadloze netwerken zijn aanvullende maatregelen aan te raden. Een veelgebruikte methode is om een extra Wireless Intrusion Prevention System (WIPS) in te richten dat zich speciaal richt op draadloze toegang tot het netwerk. Deze WIPS wordt in dat geval als buitenste schil aangebracht om bestaande beveiligingsmaatregelen als firewalls en (traditionele) IPS.

Leveranciers

AirTight Networks, Motorola (AirDefense), Cisco Systems

3.3. Controle over data en applicaties

3.3.1. Bescherming van data(opslag)

Hoewel netwerkoplossingen een bepaalde mate van veiligheid en bescherming bieden aan data, zijn er ook mogelijkheden om op dataniveau extra bescherming te bieden. Het gaat hierbij vooral om het versleutelen (en ondertekenen) van data en opslagapparaten. Daarnaast zijn er technieken om te voorkomen dat data gelekt wordt of verloren gaat. Backuptechnieken worden buiten beschouwing gelaten onder de aanname dat deze welbekend zijn en overal gebruikt worden.

Versleuteling is niets anders dan het onbegrijpelijk maken van gegevens voor anderen tenzij ze een of andere (complexe) sleutel hebben, een lange reeks karakters, waarmee de onbegrijpelijke brij weer vertaald kan worden naar de oorspronkelijke gegevens. Het versleutelen van data komt op verschillende niveaus voor. Op netwerkniveau bijvoorbeeld, wordt steeds vaker verkeer van punt A naar punt B versleuteld om te voorkomen dat de verkeersstroom onderbroken wordt en vervalst kan worden. Op deze manier kunnen ook e-mails versleuteld verstuurd worden. Op dataniveau versleutelt men gegevens met

een eigen wachtwoord zodat niemand anders behalve de gebruiker zelf bij zijn eigen gegevens kan. Op deze manier zijn ook hele harde schijven of externe opslagapparaten zoals USB-sticks te versleutelen. Wanneer een USB-stick verloren raakt, hoeft dit niet erg te zijn mits de gegevens goed genoeg versleuteld zijn. Er zijn zelfs externe opslagapparaten waarin versleuteling is ingebouwd zodat gebruikers altijd hun gegevens versleutelen.

Een andere manier om data te beschermen en dataverlies te voorkomen is het maskeren van data voor onbevoegden. Zo worden creditcard nummers online vaak (deels) gemaskeerd om te voorkomen dat meekijkers toegang krijgen tot dergelijke gegevens. Binnen organisaties kan het nodig zijn om door persoonsgegevens deels te maskeren de privacy te waarborgen.

Een belangrijke ontwikkeling zijn producten die zich specifiek richten op het voorkomen van dataverlies (Data Loss Prevention, DLP). Deze oplossingen analyseren gegevens van netwerkverkeer tot e-mails tot documenten om te bepalen of deze gegevens gevoelig zijn. Wanneer ze ontdekken dat dergelijke gegevens op openbare plekken beschikbaar zijn, kunnen ze overgaan tot filteren, blokkeren of andere methoden om te voorkomen dat de gegevens beschikbaar blijven. Hoewel deze technologie oorspronkelijk bedoeld was om te voorkomen dat data gelekt of gestolen kan worden, blijkt het ook een uitstekend middel om fouten in processen en de organisatie te ontdekken. Bovendien kunnen DLP producten worden gebruikt om te voldoen aan opgelegde normen en wetten ('compliance').

Leveranciers

Encryptie: PGP, Ironport Systems

DLP: Orechestria, Websense

3.3.2. Bescherming van databases

Overall ter wereld wordt gebruik gemaakt van databases. Zelfs de meest simpele websites gebruiken tegenwoordig vaak databases om flexibel en dynamisch hun content te kunnen presenteren. Omdat databases herkenbaar zijn opgezet en een bepaalde standaardstructuur hebben, is het mogelijk om gericht aanvallen te plaatsen op databases. Vaak worden successen behaald door fouten in de configuratie van een database (toegang, rechten, etc.) en op het detecteren van dergelijke configuratiefouten zijn de meeste producten op dit gebied ingesteld. Deze producten zijn veelal niets anders dan variaties op bestaande netwerkproducten toegepast op de specifieke omstandigheden van databases. Een andere manier van bescherming is het versleutelen van de communicatie met de database en de database gegevens zelf.

Database vulnerability scanners zijn producten die databases scannen op bekende zwakheden, veelgemaakte configuratiefouten en andere technische kwetsbaarheden. Het voordeel van dergelijke scanners ten opzichte van algemene scanners is dat ze beter bekend zijn met databasestructuren en dus dieper kunnen scannen op kwetsbaarheden.

Een volgende stap kan gemaakt worden met Database Activity Monitoring (DAM), complementair aan het scannen op kwetsbaarheden. Dit zijn producten die het databaseverkeer constant monitoren en analyseren. Het voornaamste doel van DAM is om fraude en andere vormen van misbruik van legitieme toegangsrechten te detecteren. Zo kan het bijvoorbeeld worden gebruikt om acties van gebruikers met de hoogste toegangsrechten (administrators) te blokkeren wanneer dit extreem gedrag lijkt. DAM wordt echter vooral gebruikt om toegang en verzoeken van eindgebruikers via web-applicaties te monitoren. Hierdoor kunnen zwakheden in applicaties aan het licht komen.

Het blokkeren van extreem gedrag is een eigenschap van een uitbreiding op DAMs: Database Intrusion Prevention (DBIP) producten. Deze oplossingen hebben verder de mogelijkheid om verbindingen met

gebruikers te beëindigen, opdrachten te vervangen en zaken te resetten; allerlei methoden om inbraak in een database te voorkomen. Deze manier van database bescherming is echter in ontwikkeling. Dit betekent dat men voorzichtig moet zijn met het toepassen van allerlei complexe blokkeringsregels; geadviseerd wordt het te houden bij het blokkeren van activiteiten waarvan het zonder twijfel duidelijk is dat het kwaadwillend is.

Leveranciers

Application Security, Guardium, Imperva

3.3.3. Bescherming van applicaties

Applicaties gedragen zich steeds meer als entiteiten die speciale aandacht vragen qua beveiliging, veelal geïnitieerd door rechtstreeks contact met applicaties via het internet en door 'autonoom' gedrag van applicaties zelf.

Web Application Firewalls (WAFs) zijn producten die zich als schild gedragen om applicaties te beschermen tegen misbruik. Deze bescherming is over het algemeen complementair aan firewalls op netwerkniveau omdat ze is gericht op kwetsbaarheden die door applicaties zelf zijn 'veroorzaakt'. Voorbeelden zijn configuratiefouten en kwetsbaarheden in eigengeschreven code die cross-site scripting of gedwongen URL-browsing (gebruikers worden omgeleid naar andere websites) mogelijk maken. Een WAF voorkomt dergelijk misbruik maar zal deze niet repareren.

Application Control oplossingen bepalen de rechten van een applicatie binnen een systeem. In zijn meest primitieve vorm kunnen systeembeheerders hiermee toestaan of een applicatie uitgevoerd mag worden. Een stap verder is het voorkomen van specifiek gedrag van applicaties zoals het verbieden van toegang tot het netwerk of internet tenzij ze op een whitelist staan. Het voordeel is dat vreemde applicaties niet zomaar illegaal gedrag kunnen vertonen (een geïnstalleerd virus kan niet zomaar van alles downloaden). Het nadeel is dat gebruikers zich snel beperkt voelen in hun vrijheid om zelf hun systeem te beheren.

Applicaties kunnen ten slotte nog beschermd worden door ze te testen op kwetsbaarheden middels Dynamic Application Security Testing (DAST) en Static Application Security Testing (SAST). DAST oplossingen richten zich voornamelijk op webapplicaties die continu online beschikbaar zijn. Ze zijn ontworpen om kwetsbaarheden van applicaties te ontdekken terwijl ze draaien. Hiermee wordt elk mogelijk gedrag van gebruikers die werken met de applicatie gesimuleerd. Op het moment dat applicaties worden losgelaten op het internet zijn ze vaak onvoldoende veilig en door DAST oplossingen toe te passen kan dit tot een acceptabel risico worden gereduceerd. SAST oplossingen richten zich voornamelijk op de code van de applicatie en analyseren hiermee de applicatie van binnenuit op kwetsbaarheden. SAST is voornamelijk nuttig in softwareontwikkeling waar het bij voorkeur zo vroeg mogelijk in de ontwikkelcyclus toegepast dient te worden.

Leveranciers

WAF: Barracuda Networks, Check Point Software Technologies

Application Control: Check Point Software Technologies, McAfee, Symantec

SAST: Fortify Software, HP

DAST: HP, WhiteHat Security

3.4. Raakvlakken

3.4.1. Identity management

Identity management is een onderwerp dat zeer nauw gerelateerd is aan beveiliging. Vaak wordt identity management ingezet als middel om informatiebeveiliging te verbeteren. Een rolgebaseerde infrastructuur biedt de mogelijkheid om toegang tot applicaties te beperken tot de juiste set gebruikers. Naast veiligheid levert identity management ook gebruikersgemak. Een goede infrastructuur geeft gebruikers bijvoorbeeld de mogelijkheid om plaatsonafhankelijk toegang te krijgen tot de juiste applicaties.

Op het gebied van identity management is het steeds meer de norm om authenticatie en autorisatie binnen organisaties te centraliseren. Hierdoor is het niet langer noodzakelijk voor (web)applicaties om een eigen gebruikersbestand bij te houden, waardoor beheerlasten omlaag gaan. Het wordt bijvoorbeeld makkelijker om gebruikers toe te laten of te verwijderen of ongewenste gebruikers te blokkeren omdat deze acties slechts op een plek hoeven uitgevoerd te worden. Voor gebruikers biedt centralisatie voordelen omdat ze niet bij elke nieuwe applicatie (persoons)gegevens hoeven in te voeren of bij te houden. Ook wordt single-sign-on mogelijk gemaakt: een gebruiker hoeft slechts een keer in te loggen om van meerdere applicaties gebruik te kunnen maken.

Naast het centraliseren van gebruikersrechten binnen een organisatie, is het ook mogelijk om dit over organisaties heen te doen. Dit kan voordelen bieden wanneer organisaties gebruikers uitwisselen of van dezelfde applicaties gebruik maken. Een manier om dit te doen, is om gebruik te maken van een federatie. Federatief identity management maakt het mogelijk om authenticatie- en autorisatiegegevens uit te wisselen. Een voorbeeld hiervan is de SURFfederatie. Organisaties zijn verantwoordelijk voor het beheer van hun eigen gebruikersgegevens en applicaties en delen bepaalde onderdelen met andere deelnemers van een federatie. Hierdoor worden de lasten van gebruikersbeheer verdeeld en krijgen gebruikers toegang tot nieuwe applicaties zonder dat hun organisatie kosten hoeft te maken voor het lokaal opzetten hiervan.

Een ander onderwerp binnen identity management is de manier waarop geauthenticeerd wordt. Het wordt steeds belangrijker om zeker te weten dat iemand is wie hij zegt dat hij is. Voor online handelingen is er nog niet iets vergelijkbaars als een paspoort dat in het dagelijks leven gebruikt wordt. Hoewel er nog veelvuldig gebruik wordt gemaakt van eenvoudige wachtwoorden die makkelijk te kraken zijn, worden er meer en meer nieuwe manieren en combinaties bedacht waarmee mensen zich kunnen authenticeren. Combinaties van een sterk wachtwoord en een fysieke bevestiging (biometrisch of een pasje) zijn gebruikelijk. Ook een bevestiging via een ander medium zoals mobiel (SMS) wordt veel gebruikt. Wanneer mensen online dezelfde mate van autoriteit en kritieke handelingen kunnen hebben als in het dagelijks leven, is een betrouwbare authenticatie en autorisatie onontbeerlijk om misbruik te voorkomen.

3.4.2. Processen en gedrag

Organisaties kunnen technisch alles nog zo goed op orde hebben, maar aan het eind van de rit blijft men afhankelijk van het gedrag van de medewerkers en gebruikers. Daarom zijn er vaak regels en processen in het leven geroepen om mensen te helpen op de juiste manier gebruik te maken van alle (technische) voorzieningen.

Omdat niet altijd even duidelijk is welke regels en processen aanwezig dienen te zijn en om niet telkens het wiel opnieuw uit te hoeven vinden, zijn er producten die organisaties helpen om op een bepaald

gebied tot de juiste set van afspraken en processen te komen. Het spectrum van deze producten is zeer breed. Zo biedt de IT Infrastructure Library (ITIL) handvatten om tot goede servicemanagementafspraken te komen. Ook zijn er normen en wetten die door de overheid zijn vastgesteld om organisaties te laten voldoen aan de door de samenleving gewenste veiligheid. Een voorbeeld hiervan zijn normen in de geneeskunde om privacy van patiënten te waarborgen.

Bovendien zijn er allerlei producten of manieren ontwikkeld om te toetsen hoe naar dergelijke processen geleefd wordt. Een typisch voorbeeld is een penetration test waarbij iemand middels Social Engineering-technieken probeert binnen te komen en kritieke informatie te bemachtigen. Een toetsingsmaatregel die over het algemeen niet alleen naar processen kijkt maar ook naar de techniek is het laten uitvoeren van een audit. Controle over processen en gedrag blijft echter weerbarstig. Organisaties dienen het glansrijk doorstaan van een toets dan ook niet te zien als een garantie dat alles 100% in orde is.

Het is verder belangrijk om mensen bewustzijn bij te brengen van het belang van bepaalde regels en processen. Wanneer deze niet worden nageleefd, kunnen de consequenties groot zijn. Social Engineering is de noemer van activiteiten die gebruik maken van onwetendheid of van het losjes interpreteren van regels door medewerkers. Hiermee kunnen kwaadwillenden de hand leggen op gevoelige informatie binnen een instelling. Deze kwaadwillenden kunnen zich voordoen als een reparateur, iemand van een andere afdeling of een kennis van een collega. Ook online bestaat een variant op Social Engineering die gebruik maakt van de goedgelovigheid van mensen. Het meest bekende voorbeeld is phishing, waar kwaadwillenden zich o.a. middels identieke kopieën van websites voordoen als het origineel (ze imiteren banken, webmail providers, etc.). Zodra iemand zijn gegevens heeft prijsgegeven, is het niet alleen mogelijk om die persoon schade te berokkenen, maar soms ook de organisatie die erachter zit. Niets anders dan mensen bewustmaken (middels campagnes) en wellicht enig gezond verstand kan dergelijk misbruik voorkomen.

3.4.3. Business continuity

Business continuity management (BCM) is de benaming van een verzameling activiteiten die uitgevoerd worden door een organisatie om zich ervan te verzekeren dat kritische bedrijfsfuncties beschikbaar blijven³. Voorbeelden van dergelijke activiteiten zijn projectmanagement, backups maken, een helpdesk bemannen, etc. Het gaat er dus om op welke manier een organisatie ervoor kan zorgen dat haar voornaamste functies gewaarborgd zijn en blijven, bijvoorbeeld in geval van een ramp. Uiteraard raakt dit onderwerp (informatie)beveiliging. De manier waarop beveiliging is ingericht heeft direct effect op de mate waarop continuïteit gewaarborgd is. Deze continuïteit wordt steeds vaker gevraagd door globalisering, het bedrijfskritische karakter van ICT en het 24/7 business model.

Een volwassen en succesvol BCM programma bestaat uit zes belangrijke componenten: crisismanagement, reageren op noodsituaties, herstellen van IT-rampen, voorbereid zijn op pandemieën, contingency planning en business recovery. Wanneer al deze elementen goed zijn ingevuld, ontstaat er een centrale plek in de organisatie waar alle processen gedocumenteerd zijn. Deze verzameling van informatie biedt het management de mogelijkheid om op strategisch en tactisch niveau te sturen bij de planning van activiteiten.

Er zijn verschillende producten die BCM kunnen ondersteunen en een deel van deze producten is vaak al in gebruik. Zo zijn er producten die gericht zijn op specifieke herstelwerkzaamheden zoals e-mail recovery, virtual-machine recovery en work area recovery. Andere producten zijn meer onderzoekend van aard, zoals een Business Impact Analysis. Crisismanagement kan worden ondersteund door producten die contact houden met stakeholders en de pers en die herstelwerkzaamheden en –uitgaven coördineren.

³ http://en.wikipedia.org/wiki/Business_continuity

Recente ontwikkelingen wijzen erop dat er steeds meer producten komen die het gehele BCM spectrum kunnen ondersteunen, vaak ontstaan uit traditionele producten voor herstelwerkzaamheden. Hoewel al deze producten BCM makkelijker en overzichtelijker maken, blijft BCM afhankelijk van hoe het geïntegreerd is in de organisatie. Bij veel organisaties is BCM onvoldoende ingebed om altijd adequaat te kunnen reageren op incidenten en crises. De verwachting is dat het nog enkele jaren gaat duren voordat organisaties dit goed voor elkaar hebben.

4. Rol SURFnet

SURFnet is op veel vlakken actief als het gaat om informatiebeveiliging. SURFnet dient haar netwerk en haar diensten veilig te houden, bevordert het beveiligingsbewustzijn door middel van gerichte campagnes, heeft een eigen incident response team (SURFcert) en biedt beveiligingsdiensten aan. Daarnaast zijn binnen de SURF-familie ook SURFfoundation en SURFdiensten actief op het gebied van informatiebeveiliging. Zo biedt SURFdiensten beveiligingsproducten uit de markt aan en onderhoudt SURFfoundation een community over informatiebeveiliging en beleid, SURFibo.

Het project Verkenning Beveiligingstooling is in SURFworks 2009 opgenomen met als uitgangspunt dat het gezamenlijke aanbod van beveiligingsdiensten van SURFnet en SURFdiensten niet volledige invulling biedt aan de behoeften binnen de doelgroep. Een belangrijke gedachte hierbij was dat SURFnet wellicht weinig kan toevoegen als dienst aanbieder. Op basis van het marktonderzoek dat voor dit rapport is gedaan, kan geconcludeerd worden dat de markt voor beveiligingstools dermate ontwikkeld en dynamisch is, dat SURFnet als leverancier van beveiligingstools weinig meerwaarde kan bieden, waarmee de gedachte bevestigd wordt. Dit wil niet zeggen dat SURFnet geen rol op het gebied van beveiliging heeft. Uit het rapport 'Beveiliging bij de instellingen' blijkt namelijk dat SURFnet wordt gezien als een betrouwbare partij die de kennis en expertise in huis heeft om de vraag van instellingen te kunnen beantwoorden.

In plaats van een positionering als aanbieder van beveiligingsdiensten, ligt het meer voor de hand om een kennispositie in te nemen tussen de aangesloten instellingen en de markt. De meerwaarde ligt dan in het koppelen van kennis over de markt en de techniek aan de wensen van de aangesloten instellingen. Bovendien kan vanuit deze positie in samenwerking met SURFdiensten een standaardpakket aan beveiligingstools worden samengesteld dat door SURFdiensten wordt aangeboden aan de instellingen.

De rapporten die binnen het project Verkenning Beveiligingstooling zijn opgeleverd, hebben geleid tot een set aanbevelingen voor SURFnet die in het najaar van 2009 verder onderzocht worden. Ook zal er in 2010 door SURFnet meer aandacht gegeven worden aan kennis- en expertisedeling waarbinnen beveiliging een van de belangrijke gebieden is. Onder andere door het blijven volgen van publicaties van partijen als Gartner, Forrester, andere NRENs en Educause (ECAR) wordt structurele aandacht geborgd waar het gaat om het volgen van ontwikkelingen in de markt en het beschikbaar stellen van deze kennis. Met de actuele kennis van SURFnet kan het standaardpakket dat samen met SURFdiensten wordt samengesteld ook up to date gehouden worden.