Vooronderzoek

Beveiliging tegen bedreigingen van Internet(technologie)

Versie ter inzage

Rapport

Door : Matthijs Koot

Datum : 2005-05-07

Versie : 1.0

Status : Definitief

Inhoudsopgave

Managementsamenvatting

De ICT-infrastructuur is essentieel voor de bedrijfsvoering van Univé. De financiële en CRM systemen, maar ook de hele kantoorautomatisering en aangrenzende informatiesystemen zijn noodzakelijk bij de dagelijkse activiteiten van vele medewerkers. Problemen met de infrastructuur leiden tot extra kosten en verloren productietijd. In geval van een beveiligingsprobleem zijn de gevolgen mogelijk nog ernstiger; het uitlekken van klantgegevens, aantasting van de integriteit van financiële transacties, uiteindelijk resulterend in imagoverlies en geschaad vertrouwen bij de klant.

De infrastructuur van Univé beslaat vele locaties en heeft een groeiend aantal koppelingen met externe infrastructuren, waaronder Internet. Er zijn dreigingen van zowel binnenuit als buitenaf; die dreigingen moeten worden tegengegaan om de infrastructuur – en dus de bedrijfsvoering – van Univé te beschermen. De maatregelen kunnen van verschillende aard zijn: preventief, detectief en correctief. Ter voorbereiding op een afstudeeronderzoek waarin de (vooral) detectieve maatregelen intrusion detection en logging centraal staan is een vooronderzoek uitgevoerd, waarvan dit rapport het resultaat is.

Het doel van het vooronderzoek was het krijgen van inzicht in de beveiligingsstatus van de infrastructuur. Daartoe is onderzoek gedaan naar een methode die kan worden gebruikt om dat inzicht op een voldoende abstract niveau te verschaffen. Vervolgens is die methode toegepast om een bedreiginganalyse te maken van de belangrijkste onderdelen van de infrastructuur van Univé, waarbij op basis van bureauonderzoek en interviews een beoordeling is gegeven van de genomen maatregelen.

Uit de bedreiginganalyse is gebleken dat de perimeter van Univé voldoende lijkt te zijn beveiligd, maar dat er vanwege het groeiend aantal decentraal beheerde locaties in combinatie met de voortschrijdende techniek (USB-sticks, draadloze access points, Bluetooth) een steeds grotere dreiging komt van binnenuit. Ondanks Univé-breed beleid en advies voor preventieve maatregelen op decentrale locaties kan niet worden gegarandeerd dat alle locaties zijn gevrijwaard van zulke achterdeurtjes. Toezicht en monitoring van de verschillende productieomgevingen zijn in aanvulling op de genomen preventieve maatregelen nodig om eventuele inbraken, wormen, et cetera tijdig op te merken – idealiter voordat een incident plaatsvindt.

Samenvattend kan worden gesteld dat een onderzoek naar intrusion detection/prevention en monitoring wenselijk is en dat een advies voor implementatie van zulke maatregelen bij Univé mede kan worden gebaseerd op de resultaten van dit vooronderzoek.

Dankwoord

Dit vooronderzoek is het resultaat van vijf weken onderzoek waaraan ik met veel plezier heb gewerkt. Het bureauonderzoek betrof weliswaar ‘slechts’ zelfstudie, maar voor de beoordeling van de situatie bij Univé was ik afhankelijk van de medewerking van verschillende medewerkers. Aan hen en anderen die dit vooronderzoek mede richting hebben gegeven en bereid waren om feedback te geven: allen bedankt!

Naam:	**Bedankt voor:**
Aly Agzanay	; …de rondleiding in Alkmaar
Bob Alberts	; …de feedback op het vooronderzoek
Jaco Breet	; …het interview
Paul Dekker	; …het interview
René van Dijk	; …directe ondersteuning
Egbert Dijkgraaf	; …directe ondersteuning
Liekele Hamstra	; …het interview en topologieschema’s
André Koot	; …directe ondersteuning
Jop Lopes Cardozo	; …het interview
Albert-Jan Schelhaas	; …het interview
Martin Tavenier	; …het interview
Henry Tibben	; …het interview
Rick Veenstra	; …het interview
Anno Wever	; …het interview

1. Inleiding

1.1 Onderwerp

Het onderwerp van dit (voor)onderzoek is *beveiliging van de ICT-infrastructuur van Unive*. Het onderwerp wordt beschouwd vanuit tactisch/operationeel niveau. De focus ligt op technologische bedreigingen; organisatorische bedreigingen, zoals gebrekkige procedures voor sleutelbeheer en wijzigingsbeheer, blijven – hoewel het belang ontegenzeglijk wordt erkend – in principe buiten beschouwing.

1.2 Probleemstelling

De opkomst van webtechnologie, draadloze netwerken, VPN-koppelingen en aanverwante technologie leidt bij veel organisaties tot vervaging van de grens tussen de vertrouwde netwerkperimeter en onvertrouwde netwerken. Er is daarom groeiende belangstelling voor 'deperimeterisatie' van netwerkbeveiliging, waarbij de focus verschuift naar beveiliging van de eindpunten [CompWkly1]. Bij de evolutie van beveiligingsarchitectuur is het essentieel om continu af te stemmen met de algemene ontwerpcriteria die gelden voor beveiliging (zie Bijlage 3: Ontwerpcriteria).

Imagoschade door het uitlekken van vertrouwelijke gegevens, winstderving door barbaarse aanvallen op computernetwerken en onopgemerkte fraude door malafide eindgebruikers: de bedreigingen zijn niet nieuw, maar de opmars van onvertrouwde elementen binnen bedrijfsnetwerken creëert de noodzaak om ze opnieuw te beschouwen.

Zo ook bij Univé. Als verzekeraar omgeven door eisen van de wetgever, eisen van toezichthoudende instanties en verwachtingen van verzekerden dient Univé zich bijzonder goed te kwijten van goed ingerichte preventieve en proactieve beveiligingsmaatregelen. Gartner voorspelde in 2004: *"System Downtime Caused by Software Vulnerabilities will Triple by 2008 for Firms that Don't Take Proactive Security Steps"* [Gartner1]. Eén van de onderdelen van proactieve beveiliging is het continu screenen en controleren van de eigen infrastructuur en beveiligingsarchitectuur. In aanloop op het afstudeeronderzoek waarin twee specifieke beveiligingmaatregelen centraal staan, staat in dit vooronderzoek eerst de volgende vraag centraal: tegen welk soort bedreigingen is de huidige infrastructuur van Univé nog niet voldoende beveiligd?

1.2.1 Doelstelling

Dit vooronderzoek beoogt een actuele inventarisatie van de bedreigingen die op de infrastructuur van Univé van toepassing zijn en een inschatting te geven van de mate waarin die bedreigingen zijn tegengegaan met beveiligingsmaatregelen. Die inventarisatie dient twee doelen: ten eerste creëert het een context voor het

vervolgonderzoek, ten tweede biedt het aan Security Management een overzicht van de huidige stand van zaken.

1.3 Werkwijze

De beschikbare tijd voor dit vooronderzoek (zoals gepland in het PID *Cyberdefense*) is opgesplitst in twee delen: bureauonderzoek en veldonderzoek. Uit het bureauonderzoek moet blijken met welke bedreigingen ICT-infrastructuren in het algemeen te maken hebben en hoe die vanuit tactisch niveau kunnen worden geadresseerd. Bij het veldonderzoek wordt vervolgens een inschatting gemaakt van de mate waarin de Univé infrastructuur tegen die bedreigingen is beschermd, waarbij het belangrijkste criterium voor het resultaat 'bruikbaarheid voor de organisatie' is. Een fundamentele, wetenschappelijke benadering wordt hier dus niet beoogd.

Er wordt een algemeen lagenmodel geïntroduceerd waarbinnen ICT-componenten, bedreigingen en beveiligingsmaatregelen kunnen worden geplaatst. Daarna worden per laag de verschillende categorieën van bedreigingen volgens een zelfbedachte methode beoordeeld, zodat duidelijk wordt hoe belangrijk een bepaalde categorie van bedreigingen 'in het algemeen' is. De wijze van beoordeling wordt beschreven in de inleiding van H3. Er wordt uitgegaan van *categorieën van bedreigingen*, omdat het vanwege de grote hoeveelheid aan concrete bedreigingen vrijwel onmogelijk is om elke concrete bedreiging te toetsen.

Bij het veldonderzoek is een tiental medewerkers van Univé geïnterviewd over de infrastructuur, waarna met goedkeuring van een EDP-auditor de definitieve *bedreiginganalyse*[1] is opgesteld. Bij die analyse is wederom een zelfbedachte methode gehanteerd; die methode wordt beschreven in H4.1.

Ten slotte wordt een suggestie gedaan voor eventuele aanvullende maatregelen en wordt teruggekoppeld met het vervolgonderzoek naar geconsolideerde logging en inbraakdetectie en -preventie.

[1] Er wordt dus geen *risicoanalyse* uitgevoerd; de impact die een manifestatie van de bedreiging heeft op de bedrijfsvoering van Univé (het 'afbreukrisico') blijft bijvoorbeeld buiten beschouwing – de bedrijfswaarde van de bedreigde componenten is – hoewel vanzelfsprekend relevant – geen onderwerp van het afstudeeronderzoek.

2. Principes en uitgangspunten

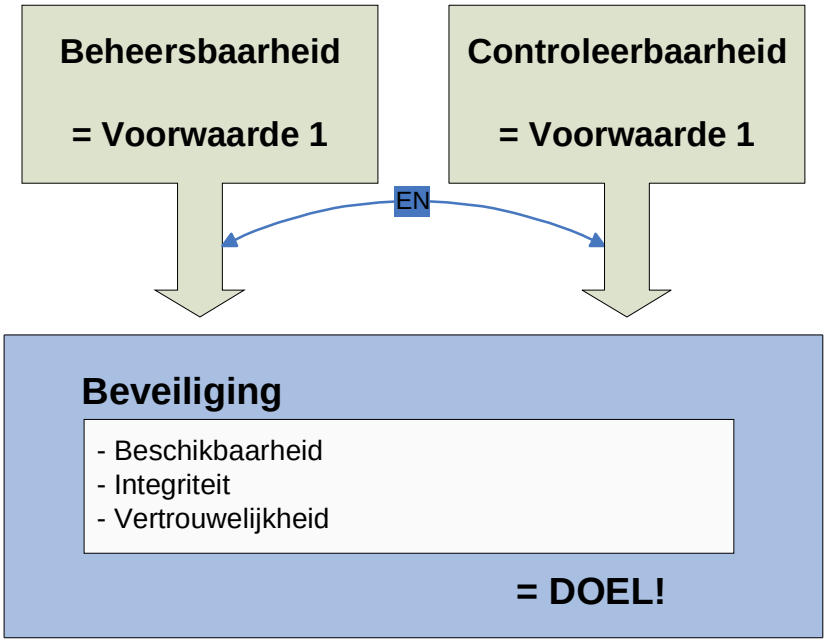
In dit hoofdstuk zal eerst een antwoord worden gegeven op de volgende vragen:

- Wat zijn de doelstellingen van informatiebeveiliging? (2.1)
- Hoe worden die doelen bedreigd? (2.2)
- Hoe kan tegen die bedreigingen worden beschermd? (2.3, 2.4)

Vervolgens zal een model worden voorgesteld waarbinnen bedreigingen en maatregelen kunnen worden geplaatst en dat als basis dient voor de bedreiginganalyse van de situatie bij Univé (2.5). De beschreven aanpak is complementair aan bestaande methoden als *threat modeling* en *attack trees* [Microsoft1], [Schneier1]; terwijl die methoden dieper ingaan op concrete bedreigingen, is de hier beschreven aanpak gericht op het snel verkrijgen van een algemeen inzicht in bedreigingen waar een ICT-infrastructuur mee te maken heeft.

2.1 Kwaliteit van informatie

Hieronder volgt een weergave van de relatie tussen de voor dit onderzoek relevante aspecten uit *Bijlage 1 – De kwaliteit van informatie*. Het is mede gebaseerd op een gesprek met André Koot.



Informatiebeveiliging is het proces dat de integriteit, beschikbaarheid en vertrouwelijkheid van informatie op een afgesproken niveau beoogt te waarborgen. Beheer(s)baarheid en controleerbaarheid zijn randvoorwaarden om informatiebeveiliging te kunnen realiseren.

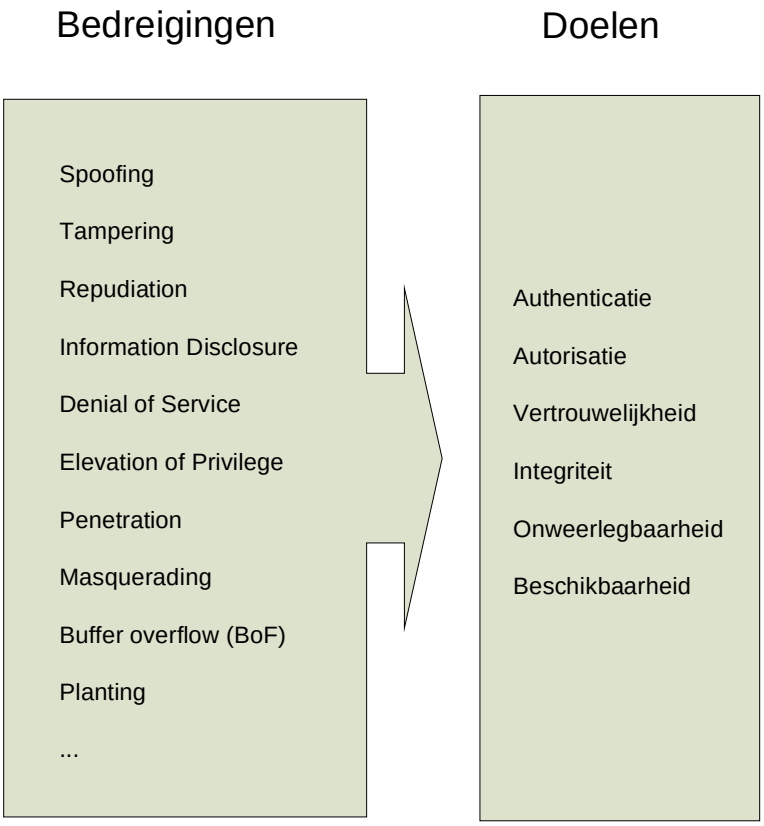
Er zouden naast beschikbaarheid, integriteit en vertrouwelijkheid (BIV) nog meer doelen kunnen worden onderscheiden [SAP1], [NIVRA1]:

- authenticatie
- autorisatie
- onweerlegbaarheid

Tegen deze fundamentele achtergronden is dit onderzoek uitgevoerd.

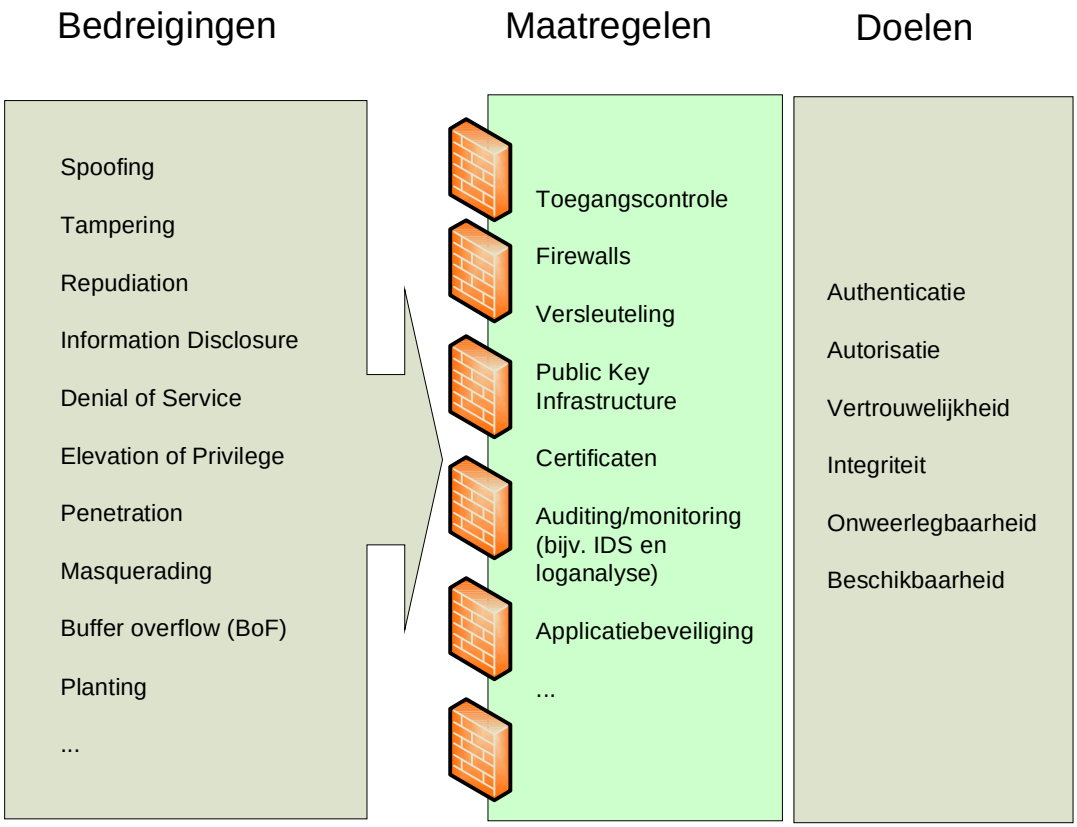
2.2 Bedreigingen en doelen

In het voorgaande hoofdstuk zijn enkele doelen van informatiebeveiliging genoemd. Er zijn diverse technologische en organisatorische bedreigingen die de doelen ondermijnen; zoals gezegd ligt de focus van dit vooronderzoek op de technologische bedreigingen. Het onderstaande schema is gebaseerd op STRIDE [Microsoft1] en aangevuld met kennis uit [SAP1]:



2.3 Beveiligingsmaatregelen

Om te voorkomen dat de doelen van informatiebeveiliging niet worden gehaald worden bedreigingen tegengegaan met beveiligingsmaatregelen:



Daarbij bestaat een veel-op-veel relatie tussen beveiligingsmaatregelen en bedreigingen; één maatregel kan meerdere bedreigingen afdekken en één bedreiging kan worden tegengegaan met meerdere maatregelen (diversiteit).

2.4 Plaatsing van maatregelen

Er worden hier drie lagen voorgesteld[2] waarop technische beveiligingsmaatregelen kunnen worden toegepast [Ham1]:

1. Netwerk
2. Host
3. Applicatie

Een ‘laag’ heeft hier twee betekenissen: enerzijds is het een groepering van logische en fysieke ICT-componenten waarop bedreigingen van toepassing zijn, anderzijds is het een mogelijke oorsprong van bedreigingen.

De **Netwerklaag** omvat in de eerste betekenis alle componenten waarmee fysieke communicatie tussen twee eindpunten wordt gefaciliteerd, zoals switches, routers en wifi access points, maar ook communicatieprotocollen. Vergelijkbaar met de vroegere ‘perimeter’. In de tweede betekenis worden er de bedreigingen mee bedoeld die afkomstig zijn van (andere) computernetwerken.

De **Hostlaag** omvat in de eerste betekenis de eindpunten van communicatie, inclusief maar niet beperkt tot servers, werkstations, PDA’s en gateways (en dan met name de besturingssystemen). In de tweede betekenis worden er de bedreigingen mee bedoeld die afkomstig zijn van (andere) hosts.

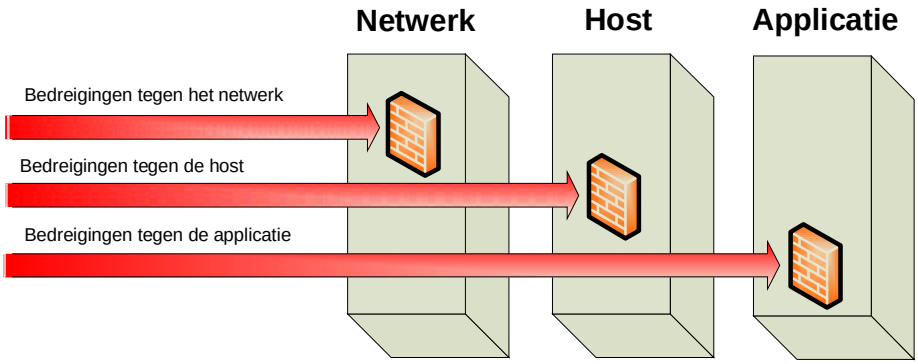
De **Applicatielaag** omvat in de eerste betekenis alle applicaties die niet tot de hostlaag kunnen of mogen worden gerekend, inclusief maar niet beperkt tot software voor webtechnologie (Apache, IIS, browsers), databases (SQL Server, MySQL, bedrijfsapplicaties), bijbehorende applicatieprotocollen en de gegevens zelf (!).In de tweede betekenis worden er de bedreigingen mee bedoeld die afkomstig zijn van (andere) applicaties.

In Bijlage 17: Technologische bedreigingen is een vrij gedetailleerd overzicht beschikbaar waarin per laag een inventarisatie is gemaakt van mogelijke bedreigingen.

Waar wordt gesproken over ‘laag’ mag ook ‘verdedigingslinie’ worden gelezen: de eerste verdedigingslinie is het netwerk, de tweede de host en de laatste de

[2] Met de intrede van middleware, component-based ontwikkeling en web services kan gepleit worden voor verdere differentiatie [Overbeek1], maar vanwege tijdsbeperking wordt in dit vooronderzoek het genoemde onderscheid gehanteerd. Een aanvullende, meer fundamentele studie zal misschien tot een ‘correcter’ inzicht leiden.

applicatie. Door maatregelen op verschillende locaties te treffen wordt *defense in depth* gerealiseerd (diversiteit):



Het belangrijkste aandachtspunt van dit vooronderzoek is netwerkbeveiliging.

Netwerk
Op deze locatie kunnen zowel fysieke als logische beveiligingsmaatregelen worden getroffen, waarbij de logische maatregelen werkzaam kunnen zijn op OSI-laag 1 t/m 7.

Voorbeelden
IPSec, firewall architecturen, auditing/monitoring

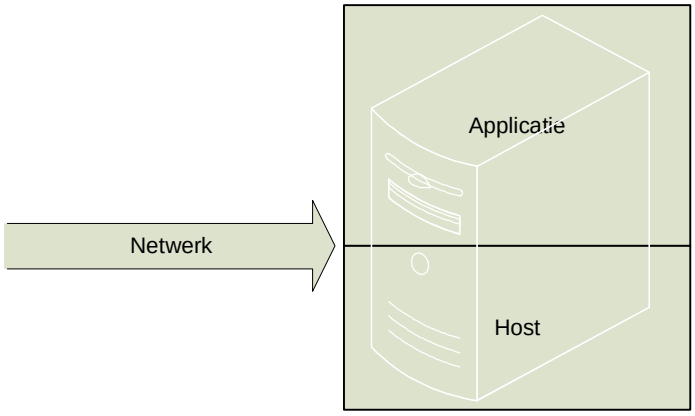
Host
Op deze locatie kunnen zowel fysieke als logische beveiligingsmaatregelen worden getroffen, waarbij de logische maatregelen werkzaam kunnen zijn op OSI-laag 1 t/m 7.

Voorbeelden
IPSec, anti-virus, resource ACLs, crypto-filesystem, auditing/monitoring

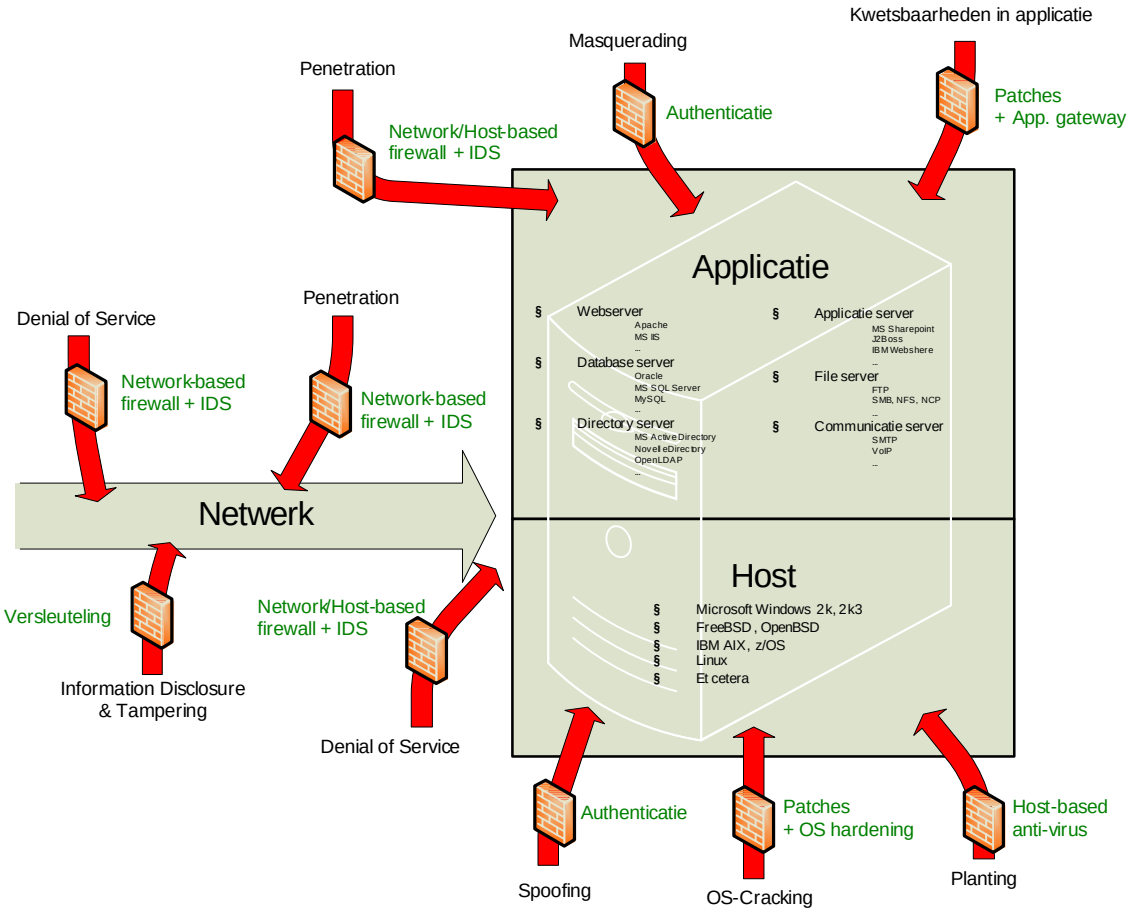
Applicatie
Op deze locatie kunnen logische beveiligingsmaatregelen worden getroffen die werkzaam kunnen zijn op OSI-laag 5 t/m 7 (aangenomen dat de applicatie gebruik maakt van de TCP/IP-stack die de host levert).

Voorbeelden
SSL, TLS, SSH tunnels, XML Encryption, XML Digital Signatures, SAML, versleuteling in database, auditing/monitoring

De lagen in een schema:

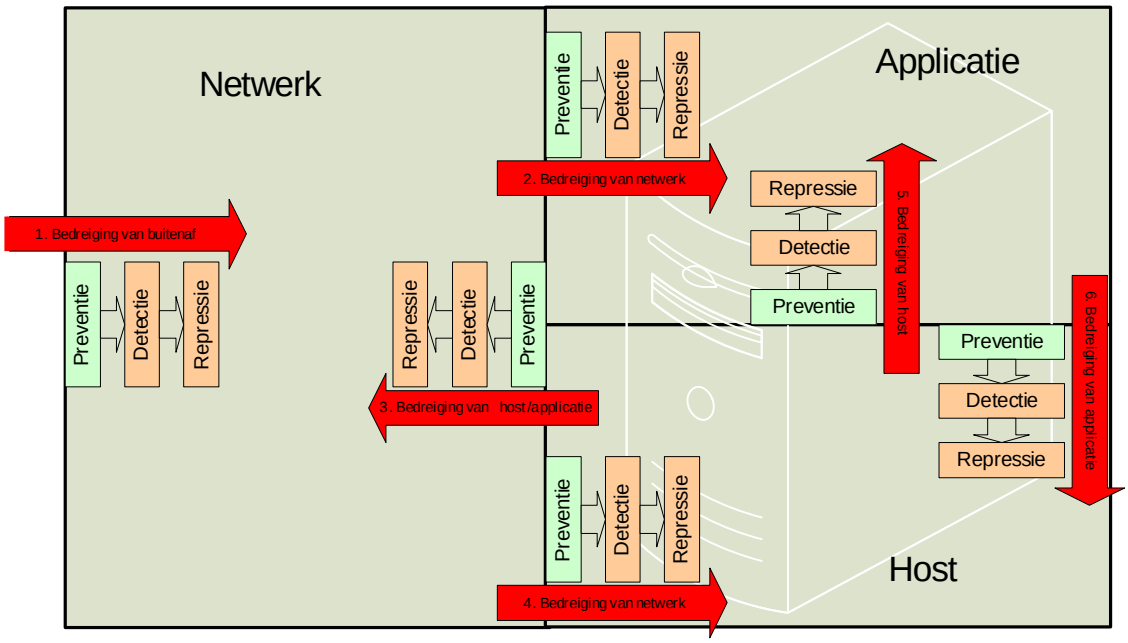


Hetzelfde schema ter illustratie uitgebreid met enkele bedreigingen en maatregelen:



2.5 Bedreigingen- en maatregelenmodel

Om inzicht te krijgen in de bedreigingen werd al een vereenvoudigd lagenmodel geïntroduceerd. Als de verschillende doelen van de maatregelen (preventie, detectie, repressie/correctie [Overbeek1]) worden samengevoegd met dat model ontstaan schema's die de basis zouden kunnen zijn voor een beveiligingsarchitectuur. Er worden twee abstractieniveaus onderscheiden.



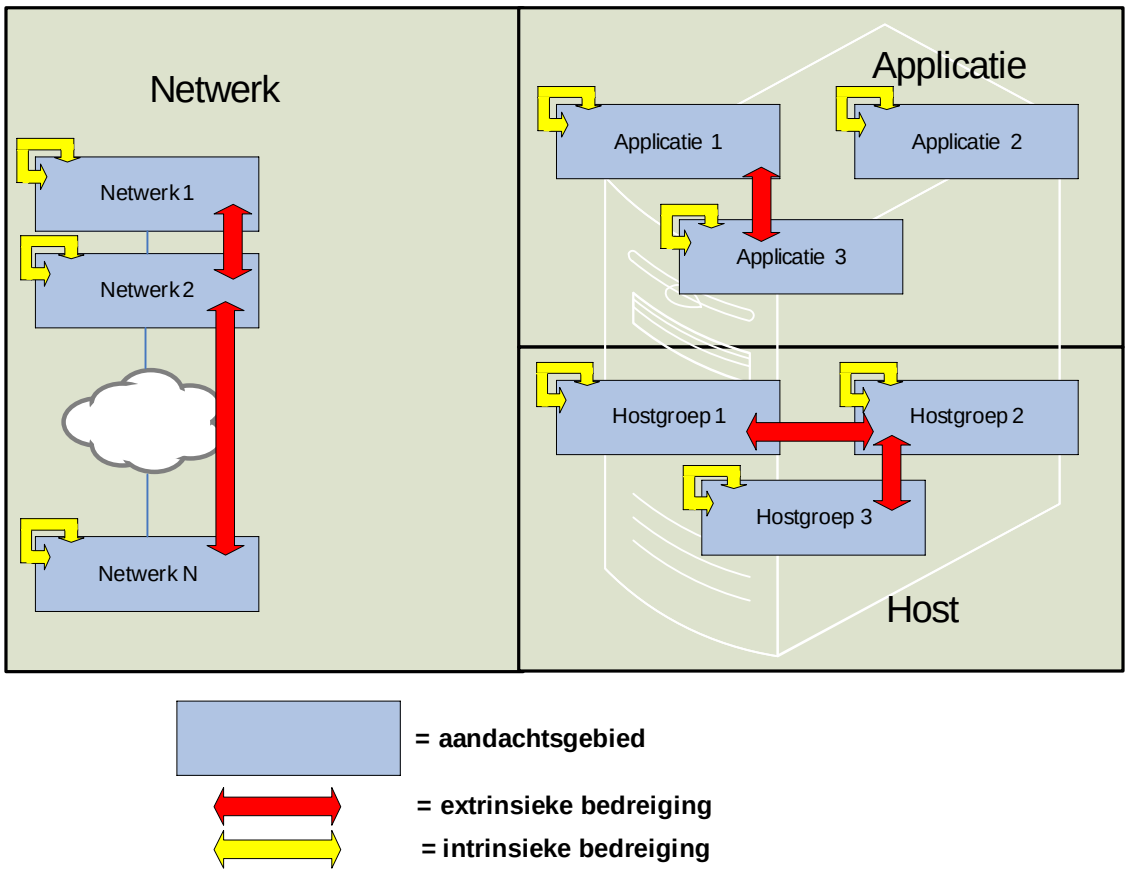
Het bovenstaande schema is een weergave van het hoogste abstractieniveau. Bij complexere infrastructuren kunnen echter per laag op basis van functionaliteit of vertrouwensniveaus verschillende aandachtsgebieden worden onderscheiden[3]. Bedreigingen die zich *binnen* zo'n aandachtsgebied afspelen worden hier *intrinsieke* bedreigingen genoemd.

Bedreigingen die 1) *tussen* verschillende aandachtsgebieden bestaan of 2) inherent zijn aan overschrijding van lagen worden *extrinsieke* bedreigingen genoemd. Laatstgenoemde was in het bovenstaande schema al zichtbaar in de vorm van rode pijlen.

Het volgende schema toont een lager abstractieniveau, waarbij de intrinsieke bedreigingen en de extrinsieke bedreigingen tussen aandachtsgebieden zichtbaar zijn. De verschillende soorten maatregelen zijn hier weggelaten.

(zie volgende pagina)

[3] Zie Bijlage 4: Domeinscheiding; de criteria voor het bepalen van de aandachtsgebieden zal per situatie en bedrijf verschillen; bruikbaarheid en begrijpelijkheid wegen waarschijnlijk zwaarder dan formele correctheid, omdat er op operationeel niveau mee moet kunnen worden gewerkt



Indien nodig kunnen natuurlijk op dezelfde manier extra abstractieniveaus worden toegevoegd aan aandachtsgebieden. In dit vooronderzoek wordt alleen uitgegaan van de genoemde abstractieniveaus.

3. Bedreigingen

In dit hoofdstuk wordt voor elke laag een aantal bedreigingen genoemd die gerelateerd zijn aan Internet(technologie). Het overzicht is zeker niet uitputtend; noch in de opsomming van bedreigingen, noch in de opsomming van beveiligingsmaatregelen om de bedreigingen tegen te gaan. Er wordt slechts een indicatie gegeven van de mogelijke bedreigingen. De eerste reden daarvoor is dat überhaupt nooit met zekerheid kan worden gesteld dat *alle* bedreigingen zijn genoemd (de factor onverwacht/onbekend: *you don't know that you don't know*). De tweede reden is de beperkte tijd die beschikbaar is voor dit vooronderzoek.

Er wordt een zelfbedachte classificatie gebruikt om een waardeoordeel uit te spreken over het risico en de actualiteit van bedreigingen:

[HOOG]	- zeer reële categorie van bedreigingen
[MIDDEL]	- reële categorie van bedreigingen
[LAAG]	- weinig reële categorie van bedreigingen

De waardering geeft aan hoe reëel (actueel, waarschijnlijk) een bepaalde categorie bedreigingen *in het algemeen* is, zonder rekening te houden met situationele omstandigheden. Elke waardering is voor een deel gebaseerd op empirische bijdragen aan de SANS Top 20[4] (daterend van 8 oktober 2004) en voor een deel op de DREAD-analyses (lees: mening) van de auteur van dit rapport, zoals in overleg met André Koot is bepaald. In het volgende hoofdstuk wordt een voorbeeld gegeven van de totstandkoming van zo'n waardeoordeel (3.1).

Na een korte beoordeling van de infrastructuur van Univé zal blijken hoe reëel de bedreigingen van een categorie in de aandachtsgebieden bij Univé zijn (4).

De categorieën zijn bepaald op grond van de aard en gevolgen van bedreigingen, zoals Microsoft beschrijft in [Microsoft1]. Elke categorie kan worden geassocieerd met typische tegenmaatregelen, waardoor het ook bij een grote infrastructuur redelijk mogelijk is om op tactisch niveau vrij snel inzicht te krijgen in eventuele ontbrekende maatregelen, zonder elke aparte bedreiging uitgebreid te beschouwen. Het gros van de bedreigingen wordt geadresseerd door voor elke laag de volgende categorieën te beschouwen: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Penetration en Eavesdropping [SAP1], [Microsoft1]. In Bijlage 17: Technologische bedreigingen is ter indicatie een aantal van de onderliggende bedreigingen opgesomd.

[4] SANS is een autoriteit op het gebied van informatiebeveiliging. Ze publiceren jaarlijks een lijst met de meest voorkomende en grootste bedreigingen.

3.1 Voorbeeld waardering

Hieronder volgt een voorbeeld van de totstandkoming van een waardeoordeel voor **Denial of Service bedreigingen vanaf het netwerk op de applicatielaag.** Dit proces is voor elke laag en categorie herhaald, maar wordt in dit rapport slechts eenmaal ter illustratie gegeven.

3.1.1 Feiten

- Op SANS staat *Web Servers & Services* als de nr. 1 kwetsbaarheid van Windows systemen.
- Op SANS staat *Web Server* als de nr. 2 kwetsbaarheid van Unix systemen.

3.1.2 Mening

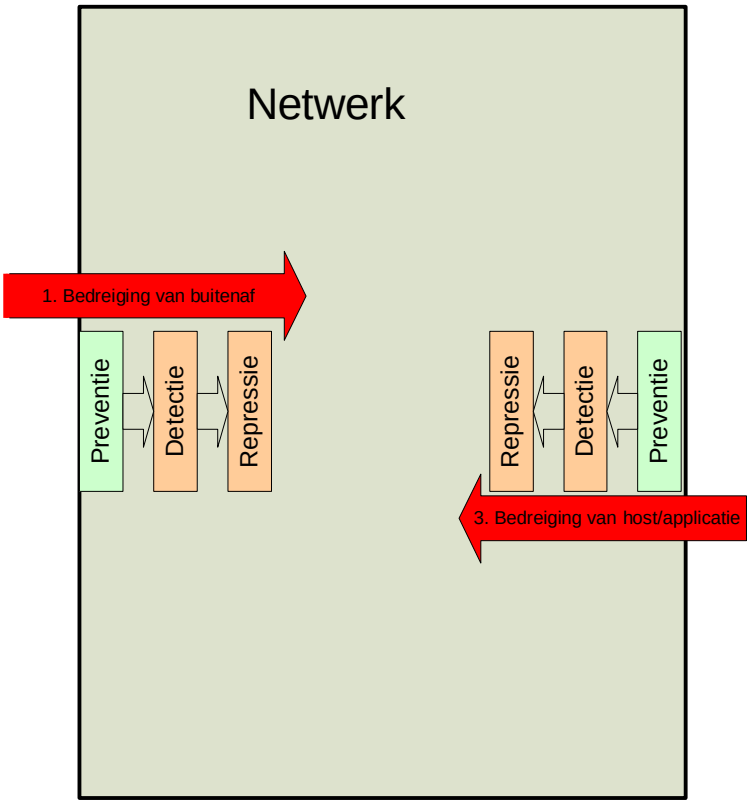
DREAD op categorie Denial of Service

- **D**amage potential is HOOG, want Denial of Service bedreigingen kunnen op publieke webdiensten leiden tot imagoverlies en derving van inkomsten uit e-commerce. Op private webdiensten kan deze bedreiging leiden tot verlies van productiviteit.
- **R**eproducability is HOOG, want Denial of Service bedreigingen kunnen worden gerealiseerd vanaf elke locatie waar de webdienst kan worden benaderd (heel Internet, bijvoorbeeld) en vereisen nauwelijks specifieke situationele omstandigheden om succesvol te kunnen worden uitgevoerd.
- **E**xploitability is HOOG, want de bedreiging is op afstand (wellicht via Internet) te realiseren, kan relatief eenvoudig worden gemaskeerd en vereist nauwelijks voorkennis.
- **A**ffected users is HOOG, want bij zowel publieke als private webdiensten worden typisch *alle* gebruikers van de dienst getroffen.
- **D**iscoverability is HOOG, want de meeste infrastructuren *zijn standaard al kwetsbaar*.

3.1.3 Conclusie

In bovenstaand voorbeeld is de applicatielaag ingevuld met *webdiensten*. Uit SANS bleek dat webdiensten tot de Top-20 van actuele kwetsbaarheden behoren. Uit DREAD bleek dat het risico in het algemeen groot is. Bij beoordeling van andere componenten die zich typisch op de applicatielaag bevinden (databasediensten, communicatiediensten) waren er vergelijkbare uitkomsten. Daarom is deze categorie van bedreigingen geclassificeerd als [HOOG].

3.2 Netwerk



Met *bedreigingen van buitenaf* worden bedreigingen vanaf zowel Internet als andere externe netwerken bedoeld, hoewel in dit vooronderzoek de focus bij Internet ligt. Onder *bedreigingen van host/applicatie* worden bedreigingen vanaf het interne netwerk geschaard.

3.2.1 Bedreigingen vanaf Internet

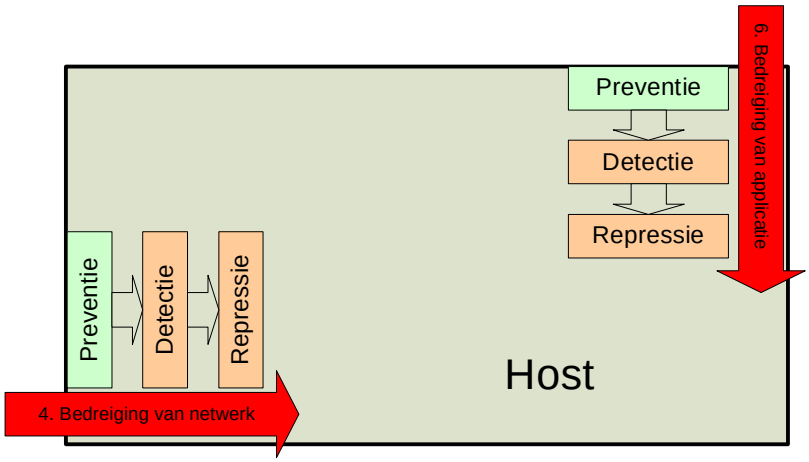
Bedreigingen vanaf Internet op de netwerklaag			
Bedreiging	**Voorbeelden**	**Algemene classificatie**	**Opmerking**
Spoofing	- IP spoofing	[LAAG]	+ eigenlijk alleen bruikbaar bij (D)DoS + makkelijk te blokkeren
Tampering	- niet-geautoriseerde update van route tabellen (BGP, RIP) - TCP hijacking	[LAAG]	+ moeilijk uitvoerbaar
Repudiation	(onbekend)	(onbekend)	
Information Disclosure	- port scanning - traceroute - subnet discovery door broadcast verzoeken - SNMP informatie	[MIDDEL]	- makkelijk uitvoerbaar + lage impact

Denial of Service	- SYN flooding DDoS - ICMP echo requests DDoS - ICMP route unreachable - malformed packets	[HOOG]	- makkelijk uitvoerbaar - hoge impact - lage pakkans
Elevation of Privilege	- VPN hacking	[LAAG]	+ moeilijk uitvoerbaar - hoge impact
Penetration	- SNMP hacking - router hacking	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact
Eavesdropping	- sniffer bij ISP	[LAAG]	+ moeilijk uitvoerbaar - hoge impact

3.2.2 Bedreigingen vanaf hosts/applicaties

Bedreigingen vanaf hosts/applicaties op de netwerklaag			
Bedreiging	**Voorbeelden**	**Algemene classificatie**	**Opmerking**
Spoofing	- IP spoofing - MAC adres spoofing	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact
Tampering	- ARP poisoning (MITM) - niet-geautoriseerde update van route tabellen (BGP, RIP) - TCP hijacking	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact
Repudiation	(onbekend)	(onbekend)	
Information Disclosure	- poortscans - traceroute - subnet discovery door broadcast verzoeken - SNMP informatie	[LAAG]	- makkelijk uitvoerbaar + lage impact
Denial of Service	- SYN flooding DDoS - ICMP echo requests DDoS - ICMP route unreachable - malformed packets	[HOOG]	- makkelijk uitvoerbaar - hoge impact + hoge pakkans
Elevation of Privilege	- VLAN hopping	[LAAG]	+ moeilijk uitvoerbaar - hoge impact
Penetration	- VLAN hopping - SNMP hacking - router hacking	[MIDDEL]	+ redelijk uitvoerbaar - hoge impact
Eavesdropping	- sniffing	[HOOG]	- makkelijk uitvoerbaar - hoge impact

3.3 Host



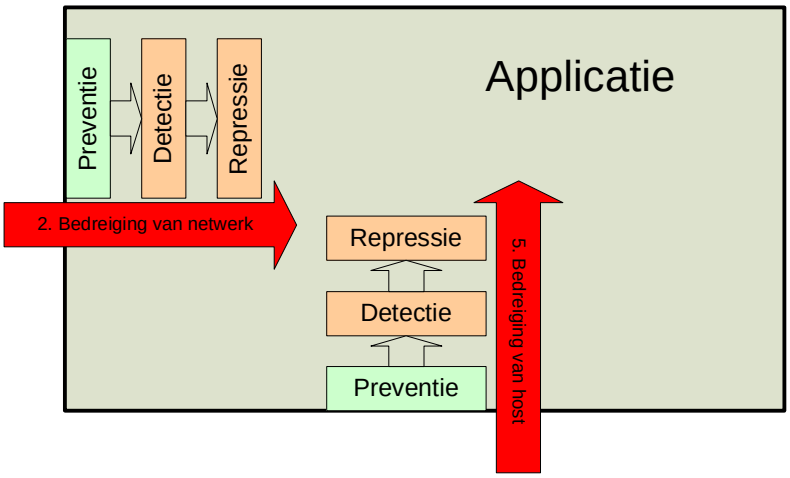
3.3.1 Bedreigingen vanaf het netwerk

Bedreigingen vanaf het netwerk op de hostlaag			
Bedreiging	**Voorbeelden**	**Algemene classificatie**	**Opmerking**
Spoofing	(onbekend)	(onbekend)	
Tampering	- OS-Cracking - malware, virussen	[HOOG]	- makkelijk uitvoerbaar - hoge impact + makkelijk te blokkeren
Repudiation	(onbekend)	(onbekend)	
Information Disclosure	- service enumeratie - poortscans - onjuiste ACLs - malware, virussen	[MIDDEL]	- makkelijk uitvoerbaar + lage impact
Denial of Service	- remote exploits	[HOOG]	+/- redelijk uitvoerbaar - hoge impact
Elevation of Privilege	- OS-Cracking - malware, virussen	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact + makkelijk te blokkeren
Penetration	- OS-Cracking	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact

3.3.2 Bedreigingen vanaf applicaties

Bedreigingen vanaf applicaties op de hostlaag			
Bedreiging	**Voorbeelden**	**Algemene classificatie**	**Opmerking**
Spoofing	(onbekend)	(onbekend)	
Tampering	(onbekend)	(onbekend)	
Repudiation	(onbekend)	(onbekend)	
Information Disclosure	(onbekend)	(onbekend)	
Denial of Service	- overbelasting van applicatie	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact
Elevation of Privilege	- uitvoeren systeemcommando's	[LAAG]	+/- redelijk uitvoerbaar +/- redelijke impact
Penetration	(onbekend)	(onbekend)	

3.4 Applicatie



3.4.1 Bedreigingen vanaf hosts

Bedreigingen vanaf hosts op de applicatielaag			
Bedreiging	**Voorbeelden**	**Algemene classificatie**	**Opmerking**
Spoofing	(onbekend)	(onbekend)	
Tampering	- schrijftoegang OS tot onversleutelde applicatiegegevens	[MIDDEL]	- makkelijk uitvoerbaar - hoge impact + toegang tot server vereist
Repudiation	- schrijftoegang tot onversleutelde applicatiegegevens (zonder via applicatie te hoeven)	[MIDDEL]	- makkelijk uitvoerbaar - hoge impact + toegang tot server vereist
Information Disclosure	- leestoegang OS tot onversleutelde applicatiegegevens	[MIDDEL]	- makkelijk uitvoerbaar - hoge impact + toegang tot server vereist
Denial of Service	- afsluiten van applicatieproces - afsluiten van afhankelijke processen - verwijderen van applicatiegegevens	[MIDDEL]	- makkelijk uitvoerbaar - hoge impact + toegang tot server vereist
Elevation of Privilege	- bij SSO: middels gekraakte OS-account toegangsrechten erven	[LAAG]	+ moeilijk uitvoerbaar + toegang tot server vereist
Penetration	- procesinjectie - brute force kraken van wachtwoorden applicatie	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact

3.4.2 Bedreigingen vanaf het netwerk

Bedreigingen vanaf het netwerk op de applicatielaag			
Bedreiging	**Voorbeelden**	**Algemene classificatie**	**Opmerking**
Spoofing	- session hijacking (HTTP cookie stelen) - session fixation	[HOOG]	- makkelijk uitvoerbaar - hoge impact
Tampering	- code injectie (SQL injectie, XPath injectie, XSS, …) - session hijacking - session fixation	[HOOG]	- makkelijk uitvoerbaar - hoge impact
Repudiation	- financiële transacties zonder handtekening - logische fouten	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact (verlaagde pakkans betekent minder risico voor de tegenstander)
Information Disclosure	- phishing - banner grabbing - over-informatieve foutmeldingen	[MIDDEL]	- makkelijk uitvoerbaar +/- redelijke impact
Denial of Service	- DDoS op applicatieniveau - remote exploits	[MIDDEL]	+/- redelijk uitvoerbaar - hoge impact
Elevation of Privilege	- code injectie (SQL injectie, XPath injectie, XSS, …) - remote exploits	[HOOG]	- makkelijk uitvoerbaar - hoge impact
Penetration	- remote exploits - code injectie (SQL injectie, XPath injectie, XSS, …)	[HOOG]	- makkelijk uitvoerbaar - hoge impact
Eavesdropping	- sniffing HTTP cookies, wachtwoorden	[HOOG]	- makkelijk uitvoerbaar - hoge impact

4. Korte bedreiginganalyse Univé

4.1 Aanpak

Om inzicht te krijgen in de situatie bij Univé is gekozen voor een aanpak die bestaat uit de volgende stappen:

1. Inventarisatie van de componenten op elke laag;
2. Inschatting van de bedreigingen die op de componenten spelen;
3. Inventarisatie van de beveiligingsmaatregelen die zijn getroffen;
4. Beoordeling van de mate waarin de bedreigingen zijn tegengegaan;
5. Conclusie met eventuele aanbevelingen.

Vanwege de grote hoeveelheid applicaties en systemen is gekozen om interviews af te nemen bij ICT-personeel; op die manier kan binnen redelijke tijd een overzicht worden gekregen van de belangrijkste componenten, zonder dat alle architectuurdocumenten hoeven worden uitgediept. Bij Univé wordt het gros van de ICT-voorzieningen voor de 150 regiokantoren gefaciliteerd vanuit het hoofdkantoor in Zwolle. Er zijn daarom in eerste instantie interviews afgenomen bij Zwols personeel. Daarnaast is er een bezoek gebracht aan de vestiging in Alkmaar, waar gesproken is met dhr. Aly Agzanay; de aantekeningen van dat bezoek zijn meegenomen in dit hoofdstuk.

Stap 4 en 5 kunnen worden uitgevoerd als de interviews voldoende informatie hebben opgeleverd. Bij de terugkoppeling wordt een oordeel geveld over de mate waarin een categorie van bedreigingen op een bepaalde laag is tegengegaan. Daarbij wordt de volgende (wederom zelfbedachte) classificatie gebruikt:

[OK]	- niet relevant, of voldoende afgedekt;
[NOK]	- relevant én onvoldoende afgedekt.

Het oordeel is deels gebaseerd op informatie uit de interviews en deels op een inschatting van de auteur van dit rapport. Alle oordelen zijn vooraf teruggekoppeld met een ervaren EDP-auditor. **De beoordeling is dus niet gebaseerd op feitelijke waarnemingen**. De uitkomst dient als achtergrond en idealiter als rechtvaardiging voor het onderzoek naar geconsolideerde logging en inbraakdetectie en -preventie.

4.2 Introductie

Het blijkt redelijk mogelijk om het voorgestelde lagenmodel (2.4) te projecteren op de beheerorganisatie van Univé. Om de situatie in kaart te brengen zijn per laag bepaalde personen geïnterviewd:

Applicatie	**à**	Martin Tavenier (senior systeemontwikkelaar) Paul Dekker (senior functioneel applicatiebeheerder - CODA) Rick Veenstra (ICT specialist – 'tooling')
Host	**à**	Jaco Breet (senior ICT specialist – Microsoft omgeving) Henry Tibben (ICT specialist – Unix/AIX omgeving) Albert-Jan Schelhaas (webmaster – technisch beheer webserver)
Netwerk	**à**	Liekele Hamstra (ICT specialist – netwerkbeheer) Jop Lopes Cardozo (ICT specialist – netwerkbeheer) Anno Wever (technisch systeembeheerder)

Enkele richtvragen:

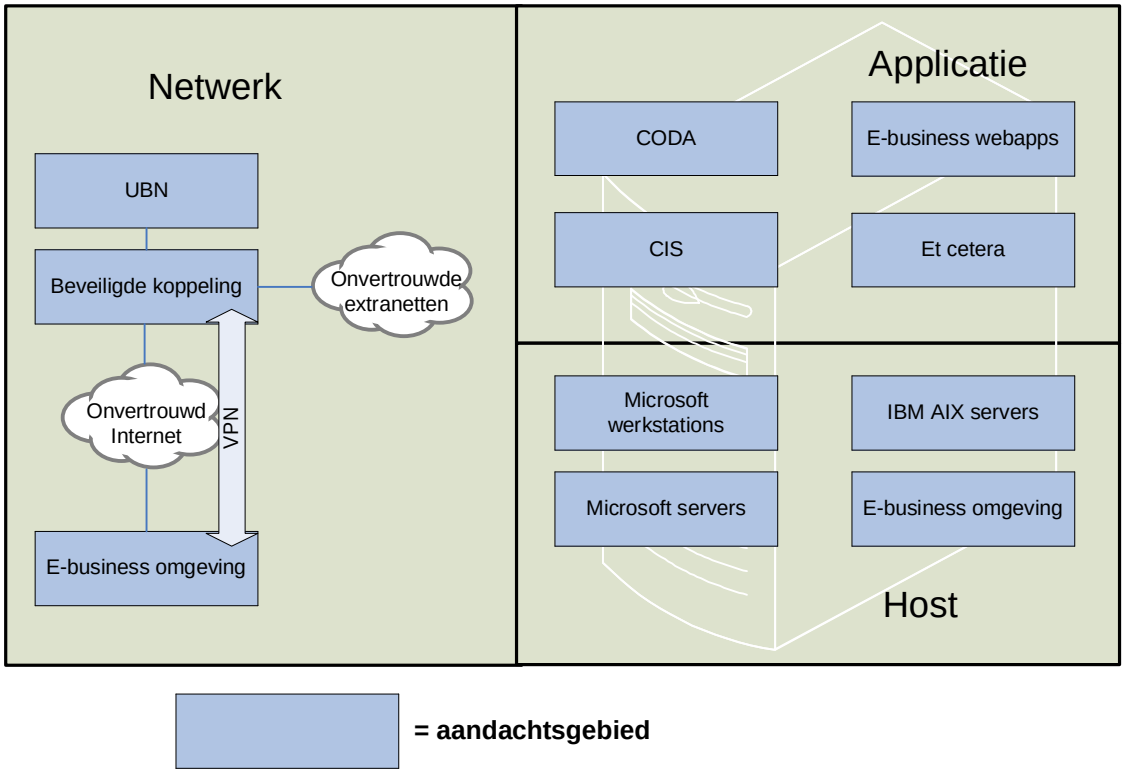
1. Wat vinden jullie belangrijk qua beveiliging (bedreigingen en maatregelen)?
2. Wat doen jullie momenteel aan beveiliging?
3. Ontbreken er maatregelen? Wat zou je meer willen doen aan beveiliging? (monitoring/logging, wellicht?)

Bij de interviews zelf hing de werkelijke vraagstelling af van het verloop van het gesprek; alle relevante informatie die bij de interviews naar voren is gekomen is vastgelegd in de bijlagen en wordt in de volgende hoofdstukken teruggekoppeld.

Bij de beoordeling van de infrastructuur van Univé in H4.5, H4.6 en H4.7 ligt de nadruk vrij expliciet op maatregelen die *ontbreken*. De maatregelen die wél zijn genomen en wellicht uitstekend beschermen tegen vele bedreigingen komen daardoor enigszins op de achtergrond. Het primaire doel van dit rapport is dan ook de *ontbrekende* maatregelen te inventariseren.

4.3 Univé in het lagenmodel

Uit de interviews en topologieschema's bleek vrij snel dat de infrastructuur van Univé zodanig heterogeen is dat het onverantwoord is om de componenten van elke laag te generaliseren (IBM AIX en Windows 2003 Server bevinden zich beide op de hostlaag, maar vanwege afwijkingen in architectuur, functionaliteit en beheer kunnen daar simpelweg geen overkoepelende oordelen over worden geveld). Daarom worden op elke laag diverse aandachtsgebieden onderscheiden en worden de beoordelingen per aandachtsgebied gegeven[5]. De aandachtsgebieden zijn in overleg met diverse medewerkers vastgesteld.



 = aandachtsgebied

Binnen elk aandachtsgebied bevinden zich componenten waarop bedreigingen spelen; routers, switches (netwerk), computers (host), MS IIS, MS SQL Server (applicaties), et cetera. Voor dit vooronderzoek – dat zich richt op beeldvorming op het tactische niveau – is het voldoende (en zelfs wenselijk) dat niet de individuele componenten worden beoordeeld, maar de groeperingen daarvan – in dit geval de bovenstaande aandachtsgebieden.

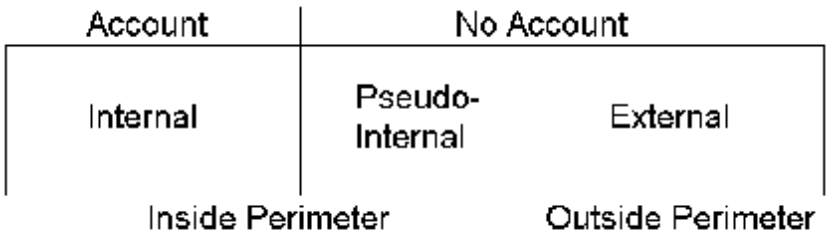
Een (vereenvoudigd) overzicht van de infrastructuur van Univé is te vinden in Bijlage 14: "De beveiligde koppeling" en Bijlage 15: Het Univé Brede Netwerk. Waar in de komende hoofdstukken wordt verwezen naar 'het interne netwerk' wordt het 'Univé Brede Netwerk' bedoeld. Dat netwerk omvat landelijk (vrijwel) alle vestigingen van Univé en betreft een klasse A subnet (10.0.0.0/8) waarbinnen –

[5] Vanwege tijdsdruk zijn niet alle aandachtsgebieden getoetst; er is echter genoeg informatie verkregen om de doelstelling van het vooronderzoek te halen. Uiteraard kan deze methode in de toekomst alsnog worden ingezet om de beveiliging van andere aandachtsgebieden te beoordelen.

met uitzondering van “de beveiligde koppeling” – geen verdere segmentering is toegepast (“Alle systemen van alle locaties kunnen elkaar pingen”).

4.4 Pseudo-internal intruders

In de komende paragrafen zal worden gesproken over bedreigingen vanaf het interne netwerk (UBN). Een belangrijke kanttekening die moet worden gemaakt is dat deze bedreigingen **niet** zijn voorbehouden aan personen met fysieke toegang tot het netwerk. De doelstellingen voor decentralisatie van het ICT-beheer naar de verschillende partijen van Univé betekenen een grotere kans op introductie van ongewenste, niet geautoriseerde ingangspunten op het UBN (draadloze netwerken, eigen Internetverbindingen) en daardoor ook op toegang van buitenaf op het UBN. Daardoor gaat er een steeds grotere dreiging uit van ‘pseudo-internal intruders’, een begrip dat Brownell Kerr Combs in zijn masterscriptie opperde om een nieuw soort tegenstanders te kenmerken [Combs1]:



The pseudo-internal intruder *is an intruder who has circumvented network perimeter defenses and gained access to the network of a distributed system without utilizing any user accounts. The primary difference between the pseudo-internal intruder and the external intruder is that the pseudo-internal intruder has completely bypassed, not broken through, any network perimeter defenses. Therefore system administrators relying solely upon network perimeter defenses to notify them of intrusions will have no knowledge of the existence of a pseudo-internal intruder.*

4.5 Netwerk

(vertrouwelijk)

4.6 Host

(vertrouwelijk)

4.7 Applicatie

(vertrouwelijk)

4.8 Conclusies

Uit de interviews blijkt dat het ICT-personeel het belang en nut van informatie-beveiliging (h)erkent. Enkele personen pleiten wel voor het scheppen van meer bewustzijn – met name onder de functionele beheerders en de eindgebruikers. Vrijwel elke geïnterviewde heeft kennis van maatregelen die zijn genomen of heeft zelf maatregelen geïmplementeerd. Ook is vrijwel iedereen het eens als het gaat om beveiliging tegen bedreigingen van buitenaf en beveiliging tegen bedreigingen van binnenuit: beide moeten in orde zijn. De meningen verschillen met name over de kans op bedreigingen van binnenuit; de één acht de huidige beveiliging voldoende, terwijl de ander op dat gebied aandringt op extra maatregelen.

In de bedreiginganalyse zijn de maatregelen verwerkt die door de geïnterviewden zijn genoemd of uit topologieschema's bleken. Wat opvalt is dat alle systemen binnen het interne netwerk – werkplekken bij regiokantoren, servers met financiële gegevens – elkaar zonder beperkingen kunnen benaderen; er is geen fijnkorrelige segmentering en er zijn alleen packet filters aanwezig bij de koppelingen richting Internet. Dat betekent dat er een ruime attack surface is voor aanvallen die van binnenuit worden geïnitieerd en gericht zijn op het UBN. Bij diverse vestigingen zijn RAS-servers in gebruik, die – hoewel ze (als het goed is) callback vereisen en langzaam zullen worden uitgefaseerd – een potentieel ingangspunt vormen op het UBN. Daarnaast komt het voor dat regiokantoren een eigen Internetverbinding hebben (ook 24x7), die – hoewel meestal in overleg met Security Management opgezet – een inherent risico met zich meebrengen. Toegang van buitenaf tot het UBN is redelijk beperkt, maar alleen de genoemde potentiële ingangspunten zijn al aanleiding genoeg om aanvullende maatregelen te nemen – zodat ongewenste toegang tijdig kan worden opgemerkt (en incidenten misschien kunnen worden voorkomen).

De medewerkers die 'wel wat zien' in geconsolideerde logging en IDS/IPS merken allen op dat baselines en inrichting van bedrijfsprocessen essentieel zijn om die maatregelen effectief te kunnen inzetten. De maatregelen introduceren in zekere zin een nieuwe 24x7 taak, waarvoor verantwoordelijkheden moeten worden belegd en personeel beschikbaar moet worden gesteld [Gartner2]. Dat is een mogelijk knelpunt; daarom is het ook het overwegen waard om andere maatregelen te overwegen waarmee dezelfde bedreigingen kunnen worden ingeperkt, zoals voorlichting over beveiliging aan de decentrale beheerders.

De systemen op het UBN zijn op netwerkniveau nauwelijks beschermd tegen bedreigingen van binnenuit en dus ook niet tegen de eerdergenoemde 'pseudo-internal intruders'; op dat gebied worden aanvullende maatregelen aanbevolen, zoals domeinscheiding (zoals segmentering van het netwerk), intrusion detection/prevention en monitoring. Samenvattend kan worden gesteld dat een vervolgonderzoek naar dergelijke maatregelen zinvol lijkt.

Begrippen

ACLs

Onder een Access Control List (ACL) wordt hier verstaan: een lijst waarmee de toegang tot een bepaalde resource kan worden beperkt. In de context *netwerkbeveiliging* gaat het meestal om toegangscontrole op basis van IP-adres en poortnummer, waarbij bijvoorbeeld geldt dat toegang tot een beheerinterface alleen is toegestaan vanaf één of enkele IP-adressen. Wanneer het gaat om een ACL in een router of firewall waarmee netwerkverkeer kan worden beperkt, wordt ook wel gesproken van *packet filter* (zie de toelichting bij *firewall*).

Anti-virus

Het ligt in de lijn der verwachting dat anti-malware zal worden geïntegreerd met anti-virus oplossingen. Omdat de aard van de bedreiging vergelijkbaar is wordt geen onderscheid gemaakt tussen beide.

Network-based

Een anti-virus appliance die topologisch tussen twee netwerkdomeinen is geplaatst en fungeert als bridge (OSI laag 2), gateway (OSI laag 3) of proxy (OSI laag 7) voor toegang tussen beide netwerken en in staat is bepaalde soorten verkeer te scannen op virussen (HTTP, FTP, SMTP, POP3, et cetera) en te blokkeren.

Host-based

Anti-virus software die op een zelfstandig systeem wordt geplaatst (server, werkstation, PDA) en alleen voor dat systeem werkzaam is. Deze vorm beschermt (in tegenstelling tot network-based) ook tegen opzettelijke of niet-opzettelijke *planting* van virussen, bijvoorbeeld via draagbare media als USB-sticks of CD-ROMs.

Anti-spam

Een appliance die topologisch tussen een SMTP server en een onvertrouwd netwerk is geplaatst, fungeert als bridge of proxy voor toegang tussen beide en in staat is inkomende (ingress) en/of uitgaande (egress) e-mail te scannen op spam. Afhankelijk van het product en configuratie-instellingen worden verschillende algoritmen gebruikt om e-mail te classificeren als spam (reikend van blacklists tot taalheuristiek) en worden berichten als spam gekenmerkt of geblokkeerd.

Attack surface

Het geheel aan ingangspunten op een beveiligingsobject of -laag dat een tegenstander potentie biedt tot het realiseren van bedreigingen.

Bedreiging

(Engels: *threat*) Een onderkend probleem dat de doelen van de informatiebeveiliging kan ondermijnen als er niets tegen wordt gedaan. Bedreigingen bestaan *altijd*, ongeacht de maatregelen die zijn genomen om ze tegen te gaan. [Microsoft1]

Beveiliging van gegevenstransport

Alle maatregelen die van toepassing zijn op de waarborging van de kwaliteitsaspecten van informatie tijdens het transport van gegevens over een computernetwerk. [NIVRA1], [Unive1]

Beveiliging van gegevensverwerking

Alle maatregelen die van toepassing zijn op de waarborging van de kwaliteitsaspecten van informatie tijdens de verwerking van gegevens binnen een computer. [NIVRA1], [Unive1]

Beveiliging van gegevensopslag

Alle maatregelen die van toepassing zijn op de waarborging van de kwaliteitsaspecten van informatie tijdens en na de opslag van gegevens in een computer. [NIVRA1], [Unive1]

Centrale logging

Hiermee wordt een systeem bedoeld waarmee uiteenlopende meldingen kunnen worden geregistreerd van gedistribueerde log-agents, zoals Windows Event Log, firewall logging, Unix syslog, logs van inbraakdetectie systemen, bedrijfsapplicaties, et cetera.

Consolidatie van logging

De gecentraliseerde aggregatie en verwerking van loggegevens uit een heterogene infrastructuur, bijvoorbeeld ten behoeve van regulier systeembeheer, maar eventueel ook specifiek ten behoeve van beveiliging.

Diversiteit

Zie ‘Gelaagde beveiliging’.

Domein

Het abstracte begrip *domein* verwijst naar een vanuit afwijking in vertrouwensniveau onderscheiden deel van een ICT-infrastructuur. In dit vooronderzoek draagt dit begrip geen formele lading, maar verwijst het bijvoorbeeld naar het onderscheid in webbrowser (ongecontroleerd) en webserver (deels of geheel gecontroleerd).

DREAD

Een methode voor de waardering van risico’s, zoals gehanteerd door Microsoft [Microsoft1]:

Damage potential	- De mate waarin een gerealiseerde bedreiging schade kan veroorzaken.
Reproducability	- De mate waarin de realisatie van een bedreiging onder gelijke omstandigheden herhaalbaar is.
Exploitability	- De mate waarin de realisatie van een bedreiging uitvoerbaar is.

Affected users	- De mate waarin de gebruikersbasis wordt getroffen door een gerealiseerde bedreiging.
Discoverability	- De mate waarin tegenstanders kwetsbaarheid voor de bedreiging kunnen ontdekken of herkennen.

Firewalls

Algemene term voor een component dat in staat is op basis van ingegeven regels netwerkverbindingen te blokkeren of door te laten. Hieronder volgt een opsomming van enkele veelgebruikte firewall architecturen.

Screening router

Bij een screened-router architectuur is een LAN alleen van Internet gescheiden door een router die op OSI laag 3 en 4 filtert:

LAN -- screening router -- Internet

Screened-host

Bij een screened-host architectuur is een LAN van Internet gescheiden door een screening router en een bastion host:

LAN -- bastion host -- screening router -- Internet

Screened-subnet

Bij een screened-subnet architectuur wordt de screened-host architectuur uitgebreid met een intern packet filter:

LAN -- intern packet filter -- bastion host -- extern packet filter -- Internet

DeMilitarized Zones (DMZ)

Een DMZ is een screened-subnet waarbij het segment tussen de twee packet filters wordt gebruikt om een extra netwerk te bouwen, meestal ten behoeve van publieke toegankelijke systemen zoals een webserver of een e-mailserver:

LAN -- intern packet filter -- LAN2 -- extern packet filter -- Internet

Gelaagde beveiliging

"Defense in depth is a concept used to describe layers of defense strategies. The components at each layer work in tandem to provide one cohesive security mechanism." [Arconati1]

Het belangrijkste doel van gelaagde beveiliging is het voorkomen van volledige compromittering van een beveiligingsarchitectuur als gevolg van het doorbreken of wegvallen van slechts één beveiligingsmaatregel. Voor dit principe wordt ook wel de term 'diversiteit' gebruikt. [Overbeek1]

Gedistribueerde beveiliging

De implementatie van één maatregel op verschillende punten in een beveiligingsarchitectuur. Zo kunnen anti-virus maatregelen bijvoorbeeld worden geïmplementeerd op zowel servers, werkstations als gateways.

Inbraakdetectie- en preventie

Network-based

Een appliance die in staat is melding te maken van bepaalde soorten ongebruikelijk of ongewenst netwerkverkeer en ofwel 1) topologisch tussen twee netwerkdomeinen is geplaatst en fungeert als bridge (OSI laag 2), gateway (OSI laag 3) of proxy (OSI laag 7) voor toegang tussen beide netwerken ofwel 2) verkeer tussen twee netwerkdomeinen kan aftappen. Als het systeem in staat is om te voorkomen dat een poging tot inbraak een eindpunt bereikt wordt ook gesproken van network-based inbraak***preventie***. Als het systeem in staat is om pas actie te ondernemen nádat een poging tot inbraak een eindpunt bereikt kan beter worden gesproken over network-based inbraak***repressie***.

Melding vindt plaats op basis van ofwel een overeenkomst tussen het netwerkverkeer en een vooraf gedefinieerde regel (***signature based***), ofwel een afwijking van het normale netwerkverkeer (***anomaly based***).

Host-based

Inbraakdetectie software die op een zelfstandig systeem wordt geplaatst (server, werkstation) en alleen voor dat systeem werkzaam is. Als het systeem in staat is om te voorkomen dat een poging tot inbraak de applicatie of het OS bereikt wordt ook gesproken van host-based inbraak***preventie***. Als het systeem in staat is om pas actie te ondernemen nádat een poging tot inbraak de applicatie of het OS bereikt kan beter worden gesproken over host-based inbraak***repressie***.

De toegevoegde waarde van host-based IDS/IPS ligt vooral in de mogelijkheid tot controle van de integriteit van het eigen systeem; network-based IDS/IPS is bijvoorbeeld niet in staat om te zien welke gevolgen bepaald netwerkverkeer werkelijk heeft (het bekende voorbeeld van een MS IIS exploit die op een Apache/Unix systeem wordt afgevuurd). Deze vorm omvat bovendien ook applicatiespecifieke IDS/IPS (bijv. een IDS/IPS agent voor MS SQL Server, mod_security voor Apache).

Kwetsbaarheid

(Engels: *vulnerability*) Een bedreiging die opzettelijk of onopzettelijk niet of onvolledig is afgedekt met beveiligingsmaatregelen.

Malicieuze code (malware)

Software die bij uitvoeren de kwaadaardige intentie van zijn ontwikkelaar realiseert. Een overkoepelende term voor virussen, wormen, spyware, exploits, et cetera.

Malware-expert Ed Skoudis pleit er voor om expliciet onderscheid te maken in verschillende soorten malware, want *"If you don't understand the differences in the categories of malicious code, you won't be able to see how specific defenses can help"*. [Skoudis1] **à** Zie Bijlage 2 – Soorten malware.

In [Gorter1] wordt een analyse gemaakt van verschillende soorten malware en wordt malware bekeken vanuit zowel een bedrijfskundig als technologisch oogpunt.

In dit vooronderzoek wordt dat onderscheid gemakshalve niet zo uitgebreid gemaakt.

STRIDE

De categorisatie van bedreigingen op basis van gevolgen, zoals gehanteerd door Microsoft [Microsoft1]:

Spoofing	- Het veinzen van een andere identiteit.
Tampering	- Het ongeautoriseerd wijzigen van gegevens of beïnvloeden van gegevensverwerking, -opslag of transport.
Repudiation	- Het in staat zijn handelingen of transacties te kunnen ontkennen (weerlegbaarheid).
Information Disclosure	- Het verstrekken van meer informatie dan noodzakelijk is voor de werking van informatievoorziening en het verlies van vertrouwelijkheid.
Denial of Service	- Het negatief beïnvloeden van beschikbaarheid van een informatievoorziening.
Elevation of Privilege	- Het door autorisatiebreuk verkrijgen van toegang tot bronnen waarvoor geen toegangsrecht is verleend.

Tegenstander

(Engels: *adversary*) Een externe entiteit, bijvoorbeeld een persoon of een stukje software, met de intentie tot het realiseren van een bedreiging. [Microsoft1]

Literatuuropgave

Bedrijfsdocumenten

[Unive1] Titel : "Informatiebeveiligingsbeleid"
Auteur(s) : drs. E. Dijkgraaf CISSP
Versie : 5.1 (2 oktober 2003)

[Unive2] Titel : "Overzicht beveiligde koppeling" (Visio document)
Auteur(s) : Liekele Hamstra
Versie : 2.2 (24 november 2004)

Vakbladen

[Gorter1] Titel : "Informatiebeveiliging" (februari 2005, maandblad GvIB)
Artikel: : "Bedrijfsmatige aanpak van Malware"
Auteur(s) : M.W. Gorter en R.C. Wannee

[NGI1] Titel : "Informatie" (januari/februari 2005, maandblad NGI)
Artikel : "Verstrekking van zekerheid als kernactiviteiten"
Auteur(s) : Ron Feijten en Wilfried Olthof

Drukwerk

[Ham1] Titel : "e-Security deel III – Internet firewalls"
Auteur(s) : A. van den Ham
Druk : 10de druk, 2005
Uitgever : International Management Forum, Eindhoven
ISBN : niet beschikbaar

[Microsoft1] Titel : "Threat Modeling"
Auteur(s) : Frank Swiderski en Window Snyder
Druk : 1ste druk, 2004
Uitgever : Microsoft Press, Redmond
ISBN : 0735619913

[NIVRA1] Titel : "Handboek EDP-auditing" (deel B, hoofdstuk B.2-01)
Auteur(s) : drs. J.J. van Beek RE RA et al
Druk : Aflevering 23 – december 2002
Uitgever : Kluwer Bedrijfswetenschappen, Deventer
ISBN : 54049502

[Overbeek1] Titel : "Informatiebeveiliging in de praktijk" (cursusmateriaal)
Auteur(s) : Dr. Ir. P.L. Overbeek RE en Dr. E. Roos Lindgreen RE
Druk : 12de druk, 2001

	Uitgever	: International Management Forum
	ISBN	: niet beschikbaar
[PI1]	Titel	: “PI-Studie Firewalls” (conceptversie)
	Auteur(s)	: Cap Gemini, André Koot RE
	Druk	: (nog niet in druk)
	Uitgever	: (nog niet in druk)
	ISBN	: (nog niet in druk)
[Skoudis1]	Titel	: “Malware – Fighting Malicious Code”
	Auteur(s)	: Ed Skoudis en Lenny Zeltser
	Druk	: 2de druk, 2004
	Uitgever	: Pearson Education / Prentice Hall, US
	ISBN	: 0131014056

Internet

[Arconati1]	Titel	: “One Approach to Enterprise Security Architecture.”
	Auteur(s)	: Nick Arconati
	Bezocht op	: 20 februari 2005
	Dateert van	: 14 maart 2002
	URI	: http://www.sans.org/rr/whitepapers/policyissues/
[Combs1]	Titel	: “The Pseudo-Internal Intruder: A New Access Oriented Intruder Category” (masterscriptie)
	Auteur(s)	: Brownell Kerr Combs
	Bezocht op	: 18 maart 2005
	Dateert van	: mei 1999
	URI	: http://www.cs.virginia.edu/~jones/IDS-research/Documents/MS-9905-Combs.doc
[CompWkly1]	Titel	: “Microsoft security chief backs users on need to ‘deperimeterise’ network security"
	Auteur(s)	: -
	Bezocht op	: 2 februari 2005
	Dateert van	: 1 februari 2005
	URI	: http://www.computerweekly.com/Article136445.htm
[Gartner1]	Titel	: “Gartner Says System Downtime Caused by Software Vulnerabilities will Triple by 2008 for Firms that Don't Take Proactive Security Steps”
	Auteur(s)	: -
	Bezocht op	: 3 maart 2005
	Dateert van	: 13 september 2004
	URI	: http://www3.gartner.com/press_releases/asset_104887_11.html

[Gartner2] Titel : "Gartner Information Security Hype Cycle: Intrusion Detection Systems"
Auteur(s) : -
Bezocht op : 1 maart 2005
Dateert van : 11 juni 2003
URI : http://www3.gartner.com/press_releases/pr11june2003c.html

[Mihai1] Titel : "Testing Malware Detectors"
Auteur(s) : Mihai Christodorescu en Somesh Jha
Bezocht op : 16 februari 2005
Dateert van : 12 juli 2004
URI : http://www.cs.wisc.edu/~mihai/my_work/papers/20040712%20-%20Testing%20Malware%20Detectors/index.html

[NextGenSS1] Titel : "Second Order Code Injection Attacks"
Auteur(s) : Gunter Ollmann
Bezocht op : 10 februari 2005
Dateert van : november 2004
URI : http://www.nextgenss.com/papers/SecondOrderCodeInjection.pdf

[Nu1] Titel : "OM onderzoekt lekken telefoontaps naar Geenstijl"
Auteur(s) : -
Bezocht op : 11 februari 2005
Dateert van : 28 januari 2005
URI : http://www.nu.nl/news.jsp?n=474708&c=50

[SANS1] Titel : "SANS Top 20 Vulnerabilities"
Auteur(s) : -
Bezocht op : 2 maart 2005
Dateert van : 8 oktober 2004
URI : http://www.sans.org/top20/

[SAP1] Titel : "Strong Infrastructure and Network Security for Heterogeneous Applications" (SCUR204)
Auteur(s) : -
Bezocht op : 26 februari 2005
Dateert van : 2003
URI : https://www.sdn.sap.com/sdn/events.sdn?page=techEd_emea.htm

[Schneier1] Titel : "Attack Trees"
Auteur(s) : Bruce Schneier
Bezocht op : 18 februari 2005
Dateert van : december 1999
URI : http://www.schneier.com/paper-attacktrees-ddj-ft.html

Bijlage 1: De kwaliteit van informatie

Citaat uit [NIVRA1]:

*"***B.2. De kwaliteit van de informatie**
De kwaliteit van een product – dus ook van informatie – is de geschiktheid van het product voor de gebruiker. Het zijn de gebruikers die de kwaliteit van de informatie vaststellen. De door deze gebruikers vastgestelde kwaliteits-/prestatie-eisen worden hier ingedeeld volgens onderstaande criteria.

De beschikbaarheid van de informatie
De beschikbaarheid van de informatie heeft betrekking op de ongestoorde voortgang van de informatievoorziening, ook wel de continuïteit genoemd. Gekozen is echter voor de term beschikbaarheid, omdat deze term beter de beschikbaarheid van informatie van uur tot uur uitdrukt.

De exclusiviteit van informatie
De exclusiviteit van informatie heeft betrekking op de beperking van de bevoegdheid en mogelijkheid tot muteren, uitlezen, kopiëren of kennisnemen (van informatie en van andere systeemcomponenten) tot een gedefinieerde groep van gerechtigden.

De integriteit van informatie
Integriteit van de informatie wil zeggen dat de informatie in overeenstemming is met het afgebeelde deel van de realiteit en dat niets ten onrechte is achtergehouden of verdwenen. In het spraakgebruik hanteert men hiervoor de termen juistheid, tijdigheid (of actualiteit) en volledigheid. (Nota bene: geoorloofdheid, ofwel autorisatie, wordt daar tegenwoordig ook bij geschaard)

De controleerbaarheid van informatie, van het informatiesysteem en van de informatievoorziening
Hierbij gaat het primair om de mogelijkheid voor de mens om vast te stellen hoe het informatiesysteem en zijn componenten zijn gestructureerd. De kwaliteit van de documentatie speelt daarbij een belangrijke rol. Verder gaat het om de mogelijkheid vast te stellen dat het proces van de gegevensverwerking en informatievoorziening tot het beoogde resultaat heeft geleid en dat gegevens en informatie (nog steeds) integer zijn. Belangrijke hulpmiddelen hiervoor zijn het omspannende controlenetwerk, standenregisters en signaleringen uit geautomatiseerde controles.

De doelmatigheid (efficiency) van de informatievoorziening
De doelmatigheid van de informatievoorziening heeft betrekking op de oplevering van de gewenste informatie (en wel tijdig) tegen aanvaardbare kosten. Bijna altijd kan meer snelheid worden verkregen door capaciteitsvergroting en dus door

kostenstijging. Als zodanig kan men efficiency ten slotte geheel als een bedrijfseconomisch probleem definiëren.

De doeltreffendheid (effectiviteit) van de informatievoorziening
Onder de doeltreffendheid van de informatievoorziening wordt verstaan de mate waarin de informatievoorziening alsook de daaraan dienstige verwerkingsprocessen aansluiten bij de verwachtingen van de informatiegebruikers.

De bescherming van waarden tegen verlies of diefstal
Bij de bescherming van waarden gaat het om materiële waarden, zoals hardware en gebouwen, maar ook om de immateriële waarden zoals kennis, researchresultaten, software e.d. De bescherming van waarden heeft juridische, organisatorische en technische aspecten, veelal van complexe aard. Voor zover het de organisatorische aspecten betreft, kan het criterium bescherming van waarden worden gerangschikt onder het criterium exclusiviteit."

Bijlage 2: Soorten malware

Definities van de verschillende soorten malware volgens [Skoudis1]:

*"A **virus** is a self-replicating piece of code that attaches itself to other programs and usually requires human interaction to propagate."*

*"A **worm** is a self-replicating piece of code that spreads via networks and usually doesn't require human interaction to propagate."*

***"Mobile code** is a lightweight program that is downloaded from a remote system and executed locally with minimal or no user intervention."*

*"A **backdoor** is a program that allows attackers to bypass normal security controls on a system, gaining access on the attacker's own terms."*

*"A **Trojan horse** is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality."*

***"RootKits** are Trojan horse backdoor tools that modify existing operating system software so that an attacker can keep access to and hide on a machine."*

Bijlage 3: Ontwerpcriteria

Citaat uit [Overbeek1], deel VII, p.9/10/11:

"Voor het toepassen en ontwerpen van technische beveiligingsmaatregelen bestaat een aantal richtlijnen of ontwerpcriteria. Een aantal van deze criteria is al in het begin van de jaren zeventig beschreven (in: Saltzer & Schroeder, 1975).

- Isolatie
  Dit principe houdt in dat hardware en software die relevant zijn voor de beveiliging – de 'Trusted Computing Base' of TCB – altijd zo klein en compact mogelijk gehouden moeten worden. Hoe groter de TCB, hoe moeilijker het zal zijn om te verifiëren of de beveiliging van de TCB voldoende gewaarborgd is. Dit principe wordt onder meer toegepast in reference monitors, security kernels en firewalls; zie hoofdstuk 5.

- Veilige defaults
  Volgens dit principe mag toegang alleen door het systeem worden verleend na expliciete permissie; alles wat niet expliciet is toegestaan, is verboden.

- Volledigheid
  Elke vorm van toegang mag pas plaatsvinden na autorisatie door het systeem. Gebruikers en processen dienen zich daartoe altijd eerst te legitimeren.

- Open ontwerp
  Een goede beveiligingsarchitectuur is niet gebaseerd op het geheimhouden van de gebruikte interne mechanismen ('security by obscurity'), maar gaat juist uit van een open ontwerp. Bij een gesloten ontwerp bestaat het risico dat de werking van internet mechanismen op den duur toch aan het licht komt, bijvoorbeeld door het toepassen van 'reverse engineering' en het uitlekken van ontwerpdocumenten. Het voordeel van een open ontwerp is bovendien dat het intensiever kan worden getest en eenvoudiger kan worden verbeterd.

- Functiescheiding
  Waar mogelijk moeten functies in het systeem worden gesplitst, waarbij de onderscheiden deelfuncties aan verschillende functionarissen moeten worden toegewezen. Gevoelige handelingen mogen alleen door meerdere functionarissen tegelijk worden uitgevoerd (het 4 ogen-principe).

- Beperking
  Het systeem moet zo opgezet zijn, dat gebruikers en processen niet meer functies mogen uitvoeren dan strikt noodzakelijk is. Dit principe staat ook bekend onder de namen 'least privilege' en 'need to know'.

- Compartimenten
  Het systeem moet bestaan uit verschillende compartimenten of modules, waarbij de koppelingen tussen de modules omwille van de controleerbaarheid zo slank mogelijk gehouden worden. Hierdoor neemt de robuustheid en daarmee ook de veiligheid van het systeem toe.

- Ergonomie
  Het systeem moet zo ontworpen zijn dat de kans op menselijke fouten zo klein mogelijk is. Beveiliging moet als het ware geïntegreerd zijn in de systemen en werkprocessen.

Daarnaast is het volgende criterium van belang.

- Redundantie
  De beveiligingsarchitectuur moet bestaan uit een combinatie van maatregelen, zodat de beveiliging niet afhankelijk is van één enkele maatregel.

Omdat men bij informatiebeveiliging niet alleen te maken heeft met onopzettelijke bedreigingen, maar ook met tegenstanders die beveiligingsmaatregelen willens en wetens proberen te omzeilen, kan dit criterium nog verder worden aangescherpt door eisen te stellen aan de diversiteit van de getroffen beveiligingsmaatregelen.

- Diversiteit
  De beveiligingsarchitectuur moet bestaan uit meerdere maatregelen die wezenlijk van elkaar verschillen, zodat het doorbreken van één beveiligingsmaatregel niet automatisch leidt tot de val van het gehele systeem."

Bijlage 4: Domeinscheiding

Intrinsieke bedreigingen

Domeinscheiding
Binnen elk laag kunnen op basis van verschil in vertrouwensniveau domeinen worden onderscheiden. Domeinen zijn in theorie onafhankelijk van domeinen op andere lagen. Zo zou een webgebaseerde bedrijfsapplicatie onderscheid kunnen maken in de vertrouwensdomeinen ‘ingelogde gebruikers’ en ‘niet-ingelogde gebruikers’ en tegelijkertijd toegankelijk zijn via zowel intranet, extranet en Internet; drie hypothetische infrastructuurdomeinen.

Domeinen kunnen echter ook samenvallen; het is aannemelijk dat in een weinig complexe organisatie hostdomeinen zouden samenvallen met netwerkdomeinen.

Voorbeeld: domeinscheiding in applicatie
Op de applicatielaag kunnen vertrouwensdomeinen worden onderscheiden op basis van applicatiespecifieke autorisatie en authenticatie van de eindgebruiker:

Domein 1 : niet-ingelogde gebruikers
Domein 2 : ingelogde gebruikers
Domein 2a : ingelogde gebruikers die de rol van ‘Beheerder’ hebben
Domein 2b : ingelogde gebruikers die niet de rol van ‘Beheerder’ hebben

Deze scheiding wordt gerealiseerd door de applicatie zelf; SAP R/3 heeft daartoe bijvoorbeeld een eigen implementatie van RBAC beschikbaar. Een overgang van het ‘niet-ingelogde gebruikers’ naar ‘ingelogde gebruikers’ dient plaats te vinden op basis van een geldige authenticatie (preventie). In alle andere gevallen is sprake van een beveiligingsincident en is de beurt aan detectieve en repressieve maatregelen op de applicatielaag (indien aanwezig).

Voorbeeld: domeinscheiding in host
Op de hostlaag kunnen vertrouwensdomeinen worden onderscheiden op basis van bedrijfsorganisatorische locatie.

Bijvoorbeeld:
Domein 1 : de business unit Schade
Domein 2 : de business unit Zorg
Domein 3 : de business unit Marketing & Verkoop

Deze domeinscheiding wordt bijvoorbeeld geïmplementeerd met directory services als Microsoft Windows’ Active Directory, Novell eDirectory en OpenLDAP.

Voorbeeld: domeinscheiding in netwerk
Op de infrastructuurlaag vallen domeinen typisch samen met netwerksegmenten.

Domein 1 : Intranet
Domein 2 : Binnenste DMZ
Domein 3 : Buitenste DMZ
Domein 4 : Internet

Deze domeinscheiding wordt bijvoorbeeld geïmplementeerd door fysieke of virtuele (802.1Q) scheiding van infrastructuren.

Bijlage 5: Kruisverwijzing onderzoeksvragen

Voorafgaand aan dit vooronderzoek zijn de onderstaande onderzoeksvragen geformuleerd.
Achter elke vraag staat het hoofdstuk waarin die vraag wordt geadresseerd.

---

1. Welke bedreigingen zijn er in het algemeen ten aanzien van ICT-infrastructuren?	H2, H3
a) Wat is informatiebeveiliging?	H2.1, H2.2, H2.3
b) Wat is een ICT-infrastructuur?	H2.4
I) Welke componenten bevinden zich in een infrastructuur?	H2.4
II) Hoe kunnen die componenten worden gegroepeerd?	H2.4
b) Welk soort bedreigingen kunnen worden onderscheiden?	H2.5, H3
c) Hoe reëel zijn die bedreigingen anno 2005?	H3
2. In hoeverre is de infrastructuur van Univé beschermd tegen die bedreigingen? (of liever: zijn geconsolideerde logging en IDS/IPS nodig?)	H4
a) Hoe ziet de infrastructuur van Univé er uit?[6]	H4.1 t/m 4.7
b) Welke maatregelen zijn er getroffen?	H4.5 t/m 4.7
c) Welke maatregelen zouden nog kunnen worden genomen?	H4.8

[6] Er zijn vanwege vertrouwelijkheid geen topologieschema's bij dit rapport opgenomen; onder andere de topologieschema's van de beveiligde koppeling in Zwolle en de infrastructuur in Alkmaar zijn geraadpleegd.

Bijlage 6 t/m 13

(vertrouwelijk)

Bijlage 14: “De beveiligde koppeling”

(vertrouwelijk)

Bijlage 15: Het Univé Brede Netwerk

(vertrouwelijk)

Bijlage 16: e-Business omgeving(en)

(vertrouwelijk)

Bijlage 17: Technologische bedreigingen

In deze bijlage wordt een opsomming gegeven van een aantal concrete technologische bedreigingen, opgesplitst in bedreigingen op de hostlaag, de applicatielaag en de netwerklaag.

Host: Werkstations

Bedreigingen t.a.v. OS

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Lokale exploits	STRIDE	- PNG bug	Host IDS	detectie	Host	
			Host IPS	repressie	Host	
			patches	preventie	Applicatie	
Malware	STRIDE	- virus - worm - wabbit - rootkit - spyware - adware - ratware - …	network firewall	preventie	Netwerk	
			host firewall	preventie	Host	
			services uitschakelen	preventie	Host	
			patches	preventie	Host	
			Network IPS	repressie	Netwerk	Voor backdoors/trojans
			Host IDS	detectie	Host	
			Network IDS	detectie	Netwerk	Voor backdoors/trojans
			anti-virus	preventie	Host	
			least privilege	preventie	Host	

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
			accounts			
			Host IPS	repressie	Host	
Open accounts (zwak of geen wachtwoord)	STRIDE	Wachtwoordloze beheerderaccount in Windows. Indien een werkstation een publiek IP-adres zou hebben en toegankelijk zou zijn vanaf Internet, kan een tegenstander (persoon, virus, enz.) de open account misbruiken.	sterk wachtwoord afdwingen	preventie	Host	
			centrale logging van inlogpogingen	detectie	Host	
Remote exploits	STRIDE	- RPC exploits - Windows Messenger spamming	Network IDS	detectie	Netwerk	
			patches	preventie	Host	
			Host IPS	repressie	Host	
			services uitschakelen	preventie	Host	
			host firewall	preventie	Host	
			Network IPS	repressie	Netwerk	
			network firewall	preventie	Netwerk	
			Host IDS	detectie	Host	

Host: Servers

Bedreigingen t.a.v. OS

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Lokale exploits	STRIDE	- PNG bug	Host IDS	detectie	Host	
			Host IPS	repressie	Host	
			patches	preventie	Applicatie	
Malware	STRIDE	- virus - worm - wabbit - rootkit - spyware - adware - ratware - …	network firewall	preventie	Netwerk	
			host firewall	preventie	Host	
			services uitschakelen	preventie	Host	
			patches	preventie	Host	
			Network IPS	repressie	Netwerk	Voor backdoors/trojans
			Host IDS	detectie	Host	
			Network IDS	detectie	Netwerk	Voor backdoors/trojans
			anti-virus	preventie	Host	
			least privilege accounts	preventie	Host	
			Host IPS	repressie	Host	
Open accounts (zwak of geen wachtwoord)	STRIDE		sterk wachtwoord afdwingen	preventie	Host	
			ACLs op beheerderaccount	preventie	Host	
			centrale logging van inlogpogingen	detectie	Host	
Remote exploits	STRIDE	- RPC exploits - Windows	Network IDS	detectie	Netwerk	

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
		Messenger spamming				
			patches	preventie	Host	
			Host IPS	repressie	Host	
			host firewall	preventie	Host	
			Network IPS	repressie	Netwerk	
			network firewall	preventie	Netwerk	
			sterk wachtwoord afdwingen	preventie	Host	
			Host IDS	detectie	Host	

Applicaties

Bedreigingen t.a.v. webbrowser

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Phishing	SI	- geldt ook voor applicaties die gebruik maken van de webbrowser (bijv. Internet Explorer in Outlook)	veilige configuratie	preventie	Applicatie	
			patches	preventie	Applicatie	

Bedreigingen t.a.v. webservers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Flooding	D	- POST requests van 64MB	Network IPS	repressie	Netwerk	
			Network IDS	detectie	Netwerk	
			patches	preventie	Applicatie	
Open beheerinterface	TIDE	- IIS Admin interface - Netscape Enterprise Server Management Console	centrale logging van wijzigingen	detectie	Applicatie	
			ACLs op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	
Remote exploits	STRIDE	- IIS exploits - Apache exploits	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			Patches	preventie	Applicatie	
			Network firewall	preventie	Netwerk	

Bedreigingen t.a.v. FTP-servers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Open accounts (zwak of geen wachtwoord)	STRIDE	- Anonymous FTP	jailed root	preventie	Applicatie	
			centrale logging van inlogpogingen	detectie	Applicatie	
			sterk wachtwoord afdwingen	preventie	Applicatie	
Remote exploits	STRIDE	- ProFTPd exploits - Microsoft FTP exploits	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			patches	preventie	Applicatie	
			network firewall	preventie	Netwerk	

Bedreigingen t.a.v. database servers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Open accounts (zwak of geen wachtwoord)	STRIDE	- elke toegang tot MS SQL Server via MS SQL Server Query Analyzer	least privilege accounts	preventie	Applicatie	
			centrale logging van inlogpogingen	detectie	Applicatie	
			sterk wachtwoord afdwingen	preventie	Applicatie	
Open beheerinterface	TIDE	- admin toegang tot MS SQL Server via MS SQL Server Enterprise Manager - admin toegang tot Oracle DBMS via Oracle Enterprise Manager	centrale logging van wijzigingen	detectie	Applicatie	
			ACLs op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	
Remote exploits	STRIDE	- MS SQL Server exploits	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			patches	preventie	Applicatie	
			network firewall	preventie	Netwerk	
Stored procedures zonder ACL	T		ACLs op aanroep	preventie	Applicatie	
			centrale logging van aanroep	detectie	Applicatie	

Bedreigingen t.a.v. DNS servers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
DNS cache poisoning	STID	- DNS server transaction ID randomization	Network IPS	detectie	Netwerk	
			veilige configuratie	preventie	Applicatie	
			Network IDS	detectie	Netwerk	
			patches	preventie	Applicatie	
Remote exploits	STRIDE	- BIND exploits - djbdns exploits	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			patches	preventie	Applicatie	
			network firewall	preventie	Netwerk	

Bedreigingen t.a.v. SMTP servers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
E-mail bom	D		ingress spam preventie	preventie	Applicatie	
			Network IPS	repressie	Netwerk	
			veilige configuratie	preventie	Applicatie	
			Network IDS	detectie	Netwerk	
Inkomende spam	T	- ‘de alledaagse spam’	ingress spam preventie	preventie	Applicatie	
Open relay	SE	- Ratware	egress spam preventie	preventie	Applicatie	
			Network IPS	repressie	Netwerk	
			veilige configuratie	preventie	Applicatie	
			Network IDS	detectie	Netwerk	
Remote exploits	STRIDE	- Sendmail exploits - MS Exchange exploits	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			patches	preventie	Applicatie	
			network firewall	preventie	Netwerk	

Bedreigingen t.a.v. webapplicaties

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
(D)HTML embedding (vorm van defacing)	TD	- HTML DIVs projecteren over legitieme FORMs	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			veilig programmeren	preventie	Applicatie	
Buffer overflow	STRIDE	Typisch het overschrijven van RET pointer door buffer overflow, met als typisch doel code executie. Bijv. een .NET webapplicatie die gebruikersinvoer zonder controle doorstuurt naar een buggy COM-object (unmanaged code).	Host IDS	detectie	Host	
			Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			veilig programmeren	preventie	Applicatie	
			Network IDS	detectie	Netwerk	
Open accounts (zwak of geen wachtwoord)	STRIDE		centrale logging van inlogpogingen	detectie	Applicatie	
			least privilege accounts	preventie	Applicatie	
			sterk wachtwoord afdwingen	preventie	Applicatie	
Open beheerinterface	STRIDE	- onbeveiligde phpMyAdmin - onbeveiligd website CMS	centrale logging van wijzigingen	detectie	Applicatie	
			ACLs op	preventie	Applicatie	

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
			beheerinterface			
			wachtwoord op beheerinterface	preventie	Applicatie	
SQL injectie (1st order and 2nd order)	TIDE	- ASP(.NET) - PHP - ColdFusion - …	Network IDS	detectie	Netwerk	
			Host IPS	repressie	Host	
			Host IDS	detectie	Host	
			Network IPS	repressie	Netwerk	
			veilig programmeren	preventie	Applicatie	
URL tampering	TIDE	- denk ook aan File Includes…	Host IDS	detectie	Host	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			ACLs op webdirectories	preventie	Applicatie	
			Network IPS	repressie	Netwerk	
			veilig programmeren	preventie	Applicatie	
XSS session hijacking	STIE	- Javascript XSS - VBScript XSS - HTTP TRACE XSS	Network IDS	detectie	Netwerk	
			Network IPS	repressie	Netwerk	
			Host IDS	detectie	Host	
			Host IPS	repressie	Host	
			veilig programmeren	preventie	Applicatie	

Netwerk: netwerkcomponenten

Bedreigingen t.a.v. switches

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
ARP flooding (switch wordt HUB)	I	Door de MAC-tabel van een switch te overflowen zal de switch overschakelen naar 'HUB-mode' en derhalve al het verkeer naar alle poorten sturen, zodat standaard promiscious mode weer voldoende is om LAN-verkeer te sniffen.	Network IPS	repressie	Netwerk	
			Network IDS	preventie	Netwerk	
ARP poisoning	STID	Door gericht ARP verkeer te genereren/onderscheppen is het mogelijk om een arbitraire omleidingsroute op te zetten, zonder dat iemand daar iets van merkt. Op die manier kan op een switched LAN verkeer worden afgeluisterd, worden platgelegd of erger nog, MITM aanvallen worden uitgevoerd (denk aan SSL MITM). Het meest voor de hand ligt het via ARP veinzen van een gateway, zodat al het verkeer dat naar de gateway zou moeten gaan naar/via de PC van de aanvaller gaat.	Network IPS	repressie	Netwerk	
			Network IDS	preventie	Netwerk	
Open beheerinterface	STRIDE	- SNMP beheerinterface - telnet beheerinterface - SSH beheerinterface - HTTP(S) beheerinterface	centrale logging van alle wijzigingen	detectie	Applicatie	
			ACLs op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	
VLAN hopping	TI	Door speciale 802.1Q pakketjes te craften is het in theorie mogelijk om jezelf voor te doen als switch en verkeer te onderscheppen dat normaal gesproken alleen via legitieme trunkpoorten wordt verstuurd. Denk daarbij aan verkeer op de management poort (VLAN1), zoals CDP en VTP advertisments.	Network IPS	repressie	Netwerk	
			Network IDS	preventie	Netwerk	

Bedreigingen t.a.v. routers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
DHCP pool exhaustion	D	Door een veelvoud aan DHCP-lease requests te sturen is het mogelijk om alle beschikbare IP-adressen op te gebruiken.	Network IPS	repressie	Netwerk	
			Network IDS	preventie	Netwerk	
Open beheerinterface	STRIDE	- SNMP beheerinterface - telnet beheerinterface - SSH beheerinterface - HTTP(S) beheerinterface	centrale logging van wijzigingen	detectie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	
Route propagatie RIP/BGP	TI	Door een 'domme' router onjuiste routeinformatie aan te bieden is het mogelijk om netwerkverkeer plat te leggen of via een arbitraire route te laten lopen.	centrale logging van geaccepteerde routeinformatie	detectie	Applicatie	
			ACLs op acceptatie van routeinformatie	preventie	Applicatie	
			Secure BGP	preventie	Applicatie	

Bedreigingen t.a.v. firewalls

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Open beheerinterface	STRIDE	- SNMP beheerinterface - telnet beheerinterface - SSH beheerinterface - HTTP(S) beheerinterface	centrale logging van wijzigingen	detectie	Applicatie	
			ACLs op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	
Pakketfragmentatie	T		Network IPS	repressie	Netwerk	
			Network IDS	preventie	Netwerk	

Bedreigingen t.a.v. NIDS/NIPS

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
IDS evasion	ST	Notatie/karaktersets (Unicode), fragmentatie van pakketjes	GEEN MAATREGEL!			
Open beheerinterface	STRIDE	- SNMP beheerinterface - telnet beheerinterface - SSH beheerinterface - HTTP(S) beheerinterface	centrale logging van wijzigingen	detectie	Applicatie	
			ACLs op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	

Bedreigingen t.a.v. printers

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Open beheerinterface	STRIDE	- SNMP beheerinterface - telnet beheerinterface - SSH beheerinterface - HTTP(S) beheerinterface	centrale logging van wijzigingen	detectie	Applicatie	
			ACLs op beheerinterface	preventie	Applicatie	
			wachtwoord op beheerinterface	preventie	Applicatie	

Netwerk: protocollen

Bedreigingen t.a.v. IP

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Source IP spoofing	S		Network IPS	repressie	Netwerk	Misschien?
			Network IDS	detectie	Netwerk	Misschien?

Bedreigingen t.a.v. TCP

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
SYN flood	D		Network IPS	repressie	Netwerk	
			Network IDS	detectie	Netwerk	
			network firewall	preventie	Netwerk	
TCP hijacking	STRIDE	Door 'educated guessing' op wat het volgende TCP sequence nummer zal zijn, kan een hacker - zelfs vanaf een ander IP - een TCP sessie overnemen. Erg ingewikkeld; afhankelijk van timing en randomization technieken en daarmee ook verschillende per TCP implementatie.	'hardened' TCP/IP stack (ivm sequence nummering)	preventie	Applicatie	
			Network IPS	repressie	Netwerk	
			Network IDS	detectie	Netwerk	

Bedreigingen t.a.v. ICMP

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
SMURF attack	D		Network IPS	repressie	Netwerk	
			Network IDS	detectie	Netwerk	
			network firewall	preventie	Netwerk	

Netwerk: overig

Bedreigingen t.a.v. Surfgedrag

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Ongewenste websites	TID	Blokkeer pornografische, racistische, illegale content / URLs	content-inspection	preventie	Netwerk	

Bedreigingen t.a.v. Instant Messaging

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Ongewenste delen van bedrijfsdocumenten	I	Tonino	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			host firewall	preventie	Host	
			network firewall	preventie	Netwerk	

Bedreigingen t.a.v. P2P

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Ongewenst delen van bedrijfsdocumenten	I	Tonino	Network IPS	repressie	Netwerk	
			Host IPS	repressie	Host	
			veilige configuratie	preventie	Applicatie	
			Network IDS	detectie	Netwerk	
			Host IDS	detectie	Host	
			host firewall	preventie	Host	
			network firewall	preventie	Netwerk	

Bedreigingen t.a.v. FTP

qryBedreigingen						
Bedreiging	**STRIDE**	**Opmerkingen**	**Maatregel**	**Doel**	**Laag**	**Notities**
Onderscheppen van plaintext authenticatie	TIE		SFTP/SCP	preventie	Applicatie	alternatief protocol gebruiken