Top 7 trends voor data- en systeembeveiliging

Met praktische voorbeelden hoe cloud computing daarbij helpt

'Wij' doen steeds meer digitaal omdat dit ons leven een stuk eenvoudiger en comfortabeler maakt. 'Wij' zijn consumenten, maar ook bedrijven, instellingen en overheden. Digitaal is eenvoudig, snel en altijd beschikbaar – op laptop, PC, telefoon en tablet. Daar waar wij steeds meer digitaal ondernemen zullen criminelen steeds vaker via een digitale weg proberen kwaad te doen. Veiligheid van systemen en informatie is daarmee voor veel organisaties topprioriteit geworden. Echter blijkt uit de praktijk[1] dat dit vaak nog grotendeels een goed voornemen is en de dagelijkse gang van zaken achterloopt op de noodzaak.

Daarbij komt bovendien dat beveiliging geen 'technisch' ding is, maar een verantwoordelijkheid van de hele organisatie. Toch wordt de IT-afdeling vaak belast met veiligheid- en privacyzaken en blijkt het lastig om andere belanghebbenden te overtuigen van nut en noodzaak van goede beveiliging. Dat vraagt om een breed ambassadeurschap digitale veiligheid en de ontwikkelingen die daarbij horen.

In dit whitepaper geven wij de 7 trends voor beveiliging van systemen en informatie en hoe cloud computing kan helpen. Voor inzicht, overzicht, controle en passende maatregelen, maar tegelijk voor het borgen van goede veiligheid binnen organisaties.

De top 7 trends voor beveiliging:

1. Afstemmen veiligheid op doelstellingen
2. Nieuwe taken voor IT
3. Dataveiligheid en risicokaders
4. Aanmelden zonder wachtwoord
5. Aanvullende veiligheidsdiensten
6. Volwassen veiligheidscompetentie
7. Continu en adaptief onderzoek

Afstemmen veiligheid op doelstellingen

Een van de belangrijkste zaken rondom veiligheid is bewustwording binnen de hele organisatie. Dit start met het management. Dit team heeft namelijk doelstellingen voor de organisatie. Om die doelstellingen te realiseren zijn acties nodig; innovatie met nieuwe producten of diensten, uitbreiding of krimp, veranderende taken en werkwijzen voor medewerkers, en zo verder. Deze acties brengen altijd risico's voor de organisatie met zich mee. Gecalculeerde risico's met financiële consequenties zijn standaard opgenomen binnen de risicoanalyse van organisaties. Maar hoewel een IT Manager of CISO[2] vaak zitting heeft in het managementteam blijkt dat er vaak onvoldoende afstemming is binnen het management en tussen het management en de rest van de organisatie.

Een groot deel is terug te leiden aan (mis)communicatie en het moeilijk kunnen vertalen van doelstellingen naar technische risico's en de bijpassende maatregelen om die risico's te verlagen. IT praat namelijk vaak digitaal, terwijl de andere managementteamleden analoog praten. Een voorbeeld:

Directeur: "Het zou voor onze bezorgers erg handig zijn als zij de klant voor ontvangst digitaal kunnen laten tekenen. Dit versnelt de administratieve afhandeling, voorkomt fouten en verhoogt de klanttevredenheid."

IT Manager: "Dat betekent dat wij applicatie X moeten ombouwen naar een App en dan op mobiele apparaten beschikbaar moeten stellen. De verbinding moet secure zijn met een SSL-certificaat en voor beveiliging is een two-factor-authentication voor de bezorger nodig."

In het bovenstaande voorbeeld is de wens voor innovatie en het optimaliseren duidelijk. Natuurlijk is het antwoord van de IT Manager in dit voorbeeld 'schetsend' opgezet, maar de praktijk ligt er niet ver vanaf. Voor het mogelijk maken van de wens zal in de techniek het nodige moeten veranderen. Vaak denkt IT direct in (beveiligings-)oplossingen. De stap die al snel overgeslagen wordt is die van het in kaart brengen van de mogelijkheden voor het technisch realiseren van de wens, de bijbehorende risico's en het hardop stellen van de vraag of techniek die risico's op moet lossen, of de 'business'.

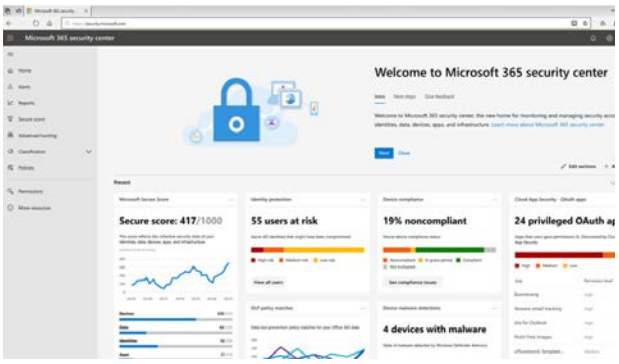
Het is slim om binnen de organisatie de digitale veiligheid integraal onderdeel te maken van zowel bedrijfsvoering als innovatie. En om diezelfde veiligheid een beslisfactor te laten zijn voor strategische beslissingen, zonder direct de technische kant van veiligheid aan te stippen.

Nieuwe taken voor IT

Veel organisaties hebben hernieuwde interesse in het Security Operations Center (SOC), ofwel een deel van de IT-afdeling dat veiligheid en beveiliging als specifieke taak heeft. Met de toenemende dreiging en de complexheid van dreigingen neemt ook het aantal oplossingen en complexheid van die oplossingen om dreiging tegen te gaan toe. Veel fabrikanten bieden slimme technologie en diensten. Om oplossingen effectief in te zetten is inzicht en overzicht van risico's en dreigingen nodig. Niet alleen 'wat te verwachten', maar ook 'live' monitoring, het opstellen van scenario's en bijpassende maatregelen.

We zien dat geïntegreerde incidentbestrijding, intelligente detectiesystemen en mogelijkheden om dreiging actief op te sporen toenemen. Cloud computing speelt daarbij een belangrijke rol. Niet alleen zijn via de cloud diverse oplossingen af te nemen en met slechts een enkele muisklik in te zetten, de cloud als basisplatform voor een veilige omgeving is steeds vaker de keuze van veel organisaties.

Zo heeft Microsoft intelligente dreigingsanalyse, Microsoft Intelligent Security Graph[4], als standaard opgenomen binnen haar publieke cloudplatform en is integraal onderdeel van zijn producten en diensten. Een snelle ontdekking van dreiging en bijbehorende acties, gebaseerd op inzicht door intelligentie, zelflerende systemen en gedragsanalyse helpen beveiligingsspecialisten bij het goed uitvoeren van hun taak. Een mooi voorbeeld daarvan zien we in het Microsoft 365 Security Center, waarvan hiernaast een voorbeeldafbeelding:



"Uit recente cijfers blijkt dat maar liefst 80% van de ondernemers met cybercrime te maken heeft gehad. Het percentage groeit elke maand. Binnen vijf jaar bevat naar verwachting meer dan 50% van de criminaliteit een digitale component. Internetcriminaliteit stijgt, in tegenstelling tot andere vormen van misdaad."

Redactie ICT Magazine, mei 2019[3]

Beveiligingsspecialist Kaspersky Lab onderzocht diefstal van wachtwoorden. Het blijkt dat in vergelijk met 2019, in de eerste helft van 2019 60% meer wachtwoorddiefstallen hebben plaatsgevonden.

Binnen één enkel portaal zijn de grootste risico's voor de organisatie, in relatie tot het gebruik van cloud computing, direct inzichtelijk en kunnen specialisten direct acties uitvoering om de veiligheid te vergroten en daarmee risico's te verlagen.

Oplossingen als deze, met ingebouwde intelligente en zelflerend vermogen, helpen bij de modernisering van het 'Security Operations Center' en tijdig klaar zijn voor toekomstige digitale dreigingen.

Dataveiligheid en risicokaders

Zoals eerder beschreven is informatiebeveiliging niet uitsluitend de verantwoordelijkheid van de IT- afdeling. Effectieve beveiliging van informatie en systemen vereist beleidskaders voor beveiliging. Dat zorgt voor een blauwdruk waarbij alles rondom informatie centraal staat. Analoog en digitaal gaan daarbij hand-in-hand. Het beleid moet leiden tot identificatie en classificatie van gestructureerde en ongestructureerde informatie binnen de hele organisatie en bepaalt uiteindelijk de veiligheidsprocedures. Zodra de strategie vanuit de organisatie bekend is en risico's in kaart gebracht zijn, kun je als organisatie prioriteiten voor investeringen in technologie bepalen.

Bij bepaald beleid hoort invoering van, en controle op dat beleid. In IT-termen en goed Engels is dat 'Governance'. Hoe borg je Governance binnen uw organisatie, zeker wanneer de organisatie cloudsystemen gaat omarmen. Microsoft heeft Governance als vast onderdeel in het Cloud Adoption Framework[5] opgenomen. Het bestaat uit een handige set aan documentatie en oplossingen rondom de methodologie voor inrichten en borgen van Governance.

Insight Enterprises heeft het Cloud Adoption Framework opgenomen binnen haar dienstverlening en kan u helpen bij het inrichten, uitvoeren en borgen van beleid rondom dataveiligheid en risicokaders.

Aanmelden zonder wachtwoord

Hoe meer systemen, hoe meer gebruikersnamen en wachtwoorden. Hoe meer wachtwoorden, hoe lastiger te onthouden. Gebruikers gaan dan ofwel vaker hetzelfde wachtwoord gebruiken, of ze kiezen voor eenvoudig te onthouden wachtwoorden. In het ergste geval schrijven ze die wachtwoorden op briefjes en plakken die onder het toetsenbord.

eid is onderdeel van de beveiligingsstrategie en daar wringt de schoen. De organisatie verlangt sterke wachtwoorden die regelmatig moeten wisselen en gebruikers willen vooral gebruiksgemak. Een van de oplossingen is een zogenaamde 'single sign on'. Dit is een oplossing waarbij gebruikers zich slechts één keer hoeven aan te melden, bijvoorbeeld op een digitale werkplek, en vanuit daar alle andere systemen benaderen. Onderhuids zijn dan alle toegangen gekoppeld aan één enkele gebruikersnaam en wachtwoord. Op zich erg gebruiksvriendelijk en technisch veilig. Maar hoe veilig is dat wanneer we naar de menselijke factor kijken?

Cybercriminelen gebruiken steeds vaker[6] slimme en geavanceerde methoden om juist bij de gebruikers hun toegangsgegevens te ontfutselen. Met die gegevens kunnen zij vervolgens bij diverse, zo niet alle systemen komen. Toegang tot systemen zonder gebruik van wachtwoorden is daarom al langer de wens van veel organisaties en beveiligingsspecialisten. Het is pas de laatste jaren dat systemen de mogelijkheid hebben om dit te ondersteunen.

Een van de mogelijkheden voor aanmelden zonder wachtwoord is gebruik maken van biometrische gegevens. Windows Hello[7], onderdeel van het Microsoft Windows besturingssysteem is een van die mogelijkheden. Windows Hello werkt op basis van gezichtsherkenning en elk gezicht heeft unieke eigenschappen. Om Hello te kunnen gebruiken moet een computersysteem, tablet of smartphone wel voorzien zijn van een camera. Een nog betere beveiliging krijgt u wanneer u de toegang tot systemen ook beveiligd via een tweetrapsverificatie. Dat betekent dat naast de biometrische gegevens een gebruiker nog een tweede methode moet inzetten om 'te bewijzen' dat hij of zij is wie hij of zij zegt. Dit kan zijn een verificatie-App op een telefoon of een USB-sleutel. Maar omgekeerd kan ook; een biometrische verificatie gebruiken als tweede methode naast een gebruikersnaam en – sterk – wachtwoord.

Microsoft Enterprise Mobility + Security is een cloud-gebaseerde oplossing die zowel beheer en beveiliging van systemen als mensen in zich heeft. Zowel Windows 10 Enterprise (voor Hello) als Enterprise Mobility + Security (meervoudige verificatie) zijn als los abonnement verkrijgbaar maar maken ook onderdeel uit van het Microsoft 365-abonnement.

Aanvullende veiligheidsdiensten

Vanwege de toenemende vraag naar beveiligingsoplossingen, software en clouddiensten is tegelijk meer gekwalificeerd personeel nodig. Echter vanwege de – wereldwijde – grote tekorten aan getraind en gecertificeerd IT-personeel zal er een groeiend gat ontstaan tussen vraag en aanbod. Tel daarbij op dat moderne veiligheidsoplossingen, gestoeld op kunstmatige intelligentie, meer menselijke interactie vragen voor het beoordelen van risico's en het nemen van maatregelen.

Door deze trend zien we steeds vaker dat leveranciers van beveiligingsoplossingen aanvullende diensten aanbieden. Denk aan het aanbieden van het product, de bijbehorende implementatie en configuratie en operationele diensten. Daarmee kunnen deze leveranciers hun klanten sneller voordeel van hun producten bieden en klanten hoeven medewerkers niet – of in elk geval – minder bij te scholen.

Een voorbeeld daarvan is het eerder beschreven Microsoft 365 Security Center, inbegrepen bij Microsoft 365-cloudabonnementen. Beheerders en beveiligingsspecialisten krijgen niet alleen scores, statussen en actuele inzichten te zien, met gebruik van intelligentie krijgen zij tegelijk aanbevelingen voor bepaalde acties. Dit voorkomt speurtochten en het leggen van verbanden tussen diverse puntoplossingen en verlaagt het benodigde kennisniveau van medewerkers om toch een afdoende beveiliging te organiseren.

Volwassen veiligheidscompetentie

Voor een volwassen veiligheidscompetentie binnen organisaties is naast kennis en kunde tegelijk inzicht, overzicht en controle nodig. Volwassen met veiligheid omgaan houdt ook in dat organisaties, wanneer zij cloud gebruiken, dat op een veilige manier moeten doen. Enkele punten om in overweging te nemen wanneer u kiest voor cloudoplossingen:

Platform
Kiest u voor cloud, dan kiest u het best voor een aanbieder met een breed platform en geïntegreerde beveiligingsoplossingen. Daarmee voorkomt u diverse cloud oplossingen met elk een eigen beveiliging, die niet op elkaar zijn afgestemd en daarmee het risico op 'gaten' in de beveiliging toelaat.

Juiste product
De basisbeveiliging is vandaag de dag goed geregeld, maar de intelligente en slimme extra's mag u zelf kiezen. Zo is Microsoft 365 E3 een bundel aan clouddiensten met standaard al extra beveiligingsopties. Kiest u daarentegen voor Microsoft 365 E5, dan kiest u voor de 'best in class' cloudoplossing voor de moderne werkplek met de hoogste mate van intelligente en adaptieve beveiliging. Belangrijk is om het te kiezen product af te stemmen op de risico's die u heeft bepaald bij Dataveiligheid en Risicokaders.

Certificering
Natuurlijk wilt u garanties, daarom kiest u het best voor een cloudplatform dat bewezen certificeringen voor veiligheid, databescherming en privacy heeft. Vergeet niet te controleren wanneer die certificeringen zijn behaald en hoe lang deze geldig zijn.

Vertrouwen
Natuurlijk, vertrouwen is goed maar controle is beter. Toch is vertrouwen in een cloudplatform, de aanbieder en de oplossingen een belangrijk gegeven voor toekomstig succes. Vertrouwen schep je door openheid en aantoonbaarheid. Insight Enterprises staat daar volledig achter en onze partner Microsoft heeft rondom het vertrouwen het 'Microsoft Trust Center' opgezet. Bezoek dat eens voor meer achtergrondinformatie en een handige 'Due diligence-controlelijst voor cloud services'[8] die u helpt bij strategische beslissingen rondom de cloud.

Ter afsluiting van dit deel, hoeveel techniek, certificeringen en vertrouwen u ook binnen uw organisatie inzet, een volwassen veiligheidscompetentie krijgt u pas wanneer veiligheid de basis is voor wat u doet binnen de hele organisatie.

Continu en adaptief onderzoek

Op de keper beschouwd is een perfecte bescherming niet mogelijk. Het spel tussen cybercriminelen en veiligheidsspecialisten gaat over en weer. Dit doet ons beseffen dat het thema beveiliging altijd en overal aanwezig moet zijn. Adaptief, dat wil zeggen 'inspelend op veranderingen.' Dit kennen we als de CARTA-strategie: Continuous Adaptive Risk and Trust Assessment. Een voortdurend onderzoek binnen én buiten de organisatie, binnen én buiten eigen of cloud IT-systemen, op zoek naar dreiging en het nemen van passende maatregelen.

Techniek kan helpen bij deze aanpak. Geïntegreerde beveiligingsoplossingen als Microsoft Advanced Threat Protection en Threat Analytics zijn goede voorbeelden. U vindt deze diensten als afzonderlijke abonnementen, of als onderdeel van bundels als Microsoft 365 en Office 365 of als toevoeging op bijvoorbeeld een SQL Database in Azure.

Interne dreiging

Naast de op de vorige pagina's beschreven top 7 trends voor data- en systeembeveiliging, die vooral gericht zijn op dreigingen van buiten, mogen we één belangrijk onderdeel niet vergeten; dreiging van binnenuit. Die dreiging onderscheiden we in twee categorieën:

- Onbedoeld (vaak bij vergissing of onwetendheid)
- Bewust

Voor beide categorieën geldt dat vooral het lekken van bedrijfsinformatie, al dan niet inclusief tot personen herleidbare informatie, het grootste deel vormt. Zeker wanneer privacygevoelige data buiten de organisatie terechtkomt zijn er grote gevolgen, zoals hoge boetes als gevolg van de strenge Algemene Verordening Gegevensbescherming (AVG).

Onderzoeksbureau Gartner[9] adviseert drie maatregelen om de interne dreiging tegen te gaan:

1. Investeer in systemen om gedrag van medewerkers te monitoren. Niet om individuen te straffen bij een 'overtreding', maar om diepgaand inzicht te krijgen in gedrag.

2. Stel profielen en persona's op om ongewoon gedrag van individuen of groepen vroegtijdig te ontdekken en maatregelen te kunnen nemen (potentieel risicogedrag).

3. Evalueer en leer van veiligheidsincidenten die een oorzaak binnen de organisatie hebben. Gebruik opgedane kennis om de voorbereiding op en acties bij incidenten te verbeteren.

Weten of uw mensen in phishing[10] e-mails trappen of op onveilige links klikken? De Attack Simulator van Microsoft geeft u de mogelijkheid gesimuleerde aanvallen op gebruikers binnen een organisatie uit te voeren. Aan de hand van de resultaten kunt u zowel het beleid als de interne communicatie aanpassen en veiligheidsbewustzijn bij medewerkers vergroten.

Kijken we naar technologie, zijn er een aantal mogelijkheden om u te helpen het risico van datalekken te verkleinen:

- Het beveiligen van identiteiten van medewerkers
- Het voorkomen dat bedrijfsdata van zakelijke naar privé e-mail gekopieerd kan worden (en ja, het is zelfs mogelijk om het maken van screenshots en het kopiëren van die screenshots te voorkomen)
- Het scheiden van zakelijke en privé Apps op mobiele apparaten van het bedrijf
- Het centraliseren van documenten en informatie waar medewerkers en eventuele externen samen aan werken
- Het beschikbaar stellen van beveiligde maar eenvoudig te gebruiken communicatiemogelijkheden, zoals zakelijke chat en videovergaderen

De hierboven beschreven maatregelen zijn als oplossing beschikbaar binnen diverse Microsoft clouddiensten, zoals Microsoft 365, Office 365 en Enterprise Mobility + Security.

Mensenwerk

Tot slot, hoeveel technologie we ook inzetten, in de kern is veiligheid een kwestie van mensenwerk. Het zijn mensen die met hun vingers aan de knoppen zitten en het zijn (grotendeels) mensen die risico's inschatten, beleid opstellen en maatregelen nemen.

Een goede adoptie van beleid en veiligheidssystemen is daarmee minstens zo belangrijk als het beleid en de systemen zelf. Want alleen wanneer medewerkers het 'waarom' van de verandering begrijpen, zullen zij hun handelen aanpassen.

Uit ervaring blijkt dat het opzetten van een adoptieprogramma, tegelijk met het opstellen van beleid – aan de hand van onderzoek – essentieel is voor succes.

Uw volgende stap

De trends zijn duidelijk. De vraag is hoe u de verwachte ontwikkelingen omzet naar concrete maatregelen voor uw organisatie. Het kan niet anders dan dat u met uw organisatie wilt blijven ontwikkelen en innoveren, maar tegelijk risico's wilt beteugelen. Om dat te realiseren stellen wij onderstaande volgende stappen voor:

1. Schrijf u in voor een **Insight en Microsoft Security Workshop**
2. Laat een (Microsoft) Cybersecurity Assessment uitvoeren door Insight Enterprises (mogelijk is daar zelfs budget vanuit Microsoft voor beschikbaar, vraag uw Insight-accountmanager naar de mogelijkheden)
3. Maak een veiligheids-aanvalsplan met heldere actiepunten en tijdlijnen
4. Start een 'proof of concept' met een geselecteerde 'workload' (bijvoorbeeld digitale werkplek, beveiliging van e-mail of werken met mobiele apparaten)
5. Migratie naar state-of-the art beveiligingsoplossingen

Over Insight.

Vandaag draait alles om technologie. Insight Enterprises Inc. geeft bedrijven van elke omvang de kracht om met Insight Intelligent Technology Solution en diensten de waarde van IT te maximaliseren. Wij zijn een wereldwijde provider van digitale innovatie, transformatie van cloud- en datacenters, een Connected Workforce en optimalisatie van de supplychain. Als Fortune 500-bedrijf helpen we klanten om hun IT vandaag succesvol in handen te nemen zodat ze volledig klaar zijn voor de toekomst. Onze meer dan 6.600 medewerkers helpen klanten om te innoveren en om hun activiteiten te optimaliseren zodat ze slimmer kunnen zakendoen.

Van IT strategie en -ontwerp tot implementatie en beheer daarvan. Ontdek meer op nl.insight.com.

1. Onderzoek Gartner naar verantwoordelijkheden voor veiligheid tijdens een bijeenkomst in juni 2019; https://www.gartner.com/smarterwithgartner/gartner-top-7-security-and-risk-trends-for-2019/
2. CISO – Chief Information Security Officer, persoon die binnen organisaties op managementniveau verantwoordelijk is voor informatiebeveiliging
3. https://www.ictmagazine.nl/grapperhaus-onderstreept-verontrustende-toename-risicos-tijdens-aftrap-landelijke-cybercrime-campagne/
4. https://www.microsoft.com/en-us/security/operations/intelligence
5. https://docs.microsoft.com/nl-nl/azure/cloud-adoption-framework/govern/
6. 60% meer wachtwoorddiefstallen in eerste helft van 2019, onderzoek door IT beveiligingsbedrijf Kaspersky Lab, augustus 2019: https://dutchitchannel.nl/628560/kaspersky-procent-meer-wachtwoorddiefstallen-in-eerste-helft-van.html
7. https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification
8. https://www.microsoft.com/nl-nl/trust-center/compliance/due-diligence-checklist
9. https://www.gartner.com/smarterwithgartner/3-ways-to-stop-insider-threats
10. Uitleg over phishing: https://nl.wikipedia.org/wiki/Phishing

MKT3979