8 CYBERSECURITY TRENDS VAN 2018

Door Rob van der Staaij en Jelger Groenland

Een exponentiele groei in de hoeveelheid digitale interacties en data, in combinatie met nieuwe wetgeving zoals GDPR, PSD2 en eIDAS, zorgt ervoor dat organisaties nog kritischer moeten kijken naar hun cybersecurityaanpak. Acht cybersecuritytrends die geen enkele organisatie mag missen.

1.

Klanten krijgen meer controle over eigen data

Zodra in mei 2018 de Algemene Verordening Gegevensbescherming (AVG of in het Engels GDPR) in werking treedt, krijgen klanten meer invloed op welke van hun persoonlijke gegevens organisaties mogen verwerken. Organisaties moeten in kaart brengen wie hun klanten zijn, welke persoonlijke klantgegevens beschikbaar zijn en hoe het gesteld is met de expliciete toestemming om bepaalde data op te slaan en te verwerken.

Verlies van data of het niet voldoen aan de eisen van dataverwerking kan resulteren in hoge boetes. Hierdoor wordt het economisch interessant om klanten zelf meer controle te geven over persoonlijke gegevens en hen eenvoudig toestemming te laten geven (en intrekken) voor het gebruik ervan. Door de controle aan de klant terug te geven, bijvoorbeeld via een onlineportal, zorgt de organisatie ervoor dat deze informatie altijd up-to-date is. Hierdoor neemt het risico van onjuist gebruik af en ontstaat er meer vertrouwen bij de klant.

Een voorbeeld: Burgers krijgen straks meer controle over hun medische gegevens via het MedMij-afsprakenstelsel. Het grote voorbeeld hierin is Estland waar men ver gevorderd is met e-health. We kunnen veel meer van dit soort initiatieven verwachten dit jaar.

2.

Toename in digitale identiteiten en ontzuiling in het managen ervan

Door de grote digitaliseringsgolf blijft het aantal digitale identiteiten toenemen. De traditionele verzuilde manier van identity- & accessmanagement, waarbij vrijwel alleen aandacht is voor de interne medewerker en er een ander systeem is voor de klanten, voldoet daarom niet meer.

We zien dan ook dat steeds meer leveranciers van technische IAM-oplossingen het managen van medewerker- en klantidentiteiten combineren. Daarnaast wordt het managen van machine-identiteiten van bijvoorbeeld slimme apparaten of andere applicaties ook opgepakt. Nieuwe IAM-oplossingen zijn al in staat om medewerkers, klanten en machines onder te brengen op één platform. De volgende stap is het gebruikmaken van gevalideerde publieke identiteitsdiensten met een hoog betrouwbaarheidsniveau (zoals bijvoorbeeld eHerkenning, IDIN, et cetera). Met de uitrol van de eIDAS-regelgeving – Europese burgers en bedrijven moeten vanaf 29 september 2018 bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met een door Europa erkend nationaal inlogmiddel – is de verwachting dat dit in Europa verder zal versnellen.

3.

Toename gebruik encryptie en hashingtechnologie

Alhoewel de technologie op zichzelf niet nieuw is, zien wij een toename in gebruik en interesse in cryptografische beheerstechnieken.

IN 2018 WORDT SERIEUS WERK GEMAAKT VAN HET STANDAARDISEREN VAN API-BEVEILIGING

De eerste ontwikkeling die daartoe leidt, is de opslag van steeds meer data buiten de grenzen van de organisatie, zoals bijvoorbeeld bij de cloudservices. Doordat steeds meer data buiten de organisatie wordt opgeslagen, neemt de noodzaak voor goede versleuteling toe. De tweede ontwikkeling die bijdraagt aan de groeiende interesse in encryptie en hashingtechnologie, is de Europese verordening AVG. Door te zorgen voor juiste encryptie van persoonsgegevens is er in het geval van een datalek geen noodzaak meer om elk datasubject individueel in te lich-

ten. Dit scheelt potentieel hoge kosten. Als laatste heeft de toename van blockchain-toepassingen, zoals cryptocurrencies, blockchain-identities en smart contracts, impact op de interesse voor hashingtechnologie. Voor het borgen van de authenticiteit en de integriteit van de blockchaingegevens is zowel encryptie als hashing van uitermate groot belang.

4.

Standaardisatie van api-beveiliging

Er is sprake van een versnelde toename in het gebruik van api's, niet in de laatste plaats aangejaagd door de transitie naar DevOps, de opkomst van de *composable enterprise* en meer regeldruk (PSD2). Met die toename nemen ook de zorgen over de veiligheid toe.
Er valt dan ook te voorzien dat in 2018 serieus werk wordt gemaakt van het standaardiseren van api-beveiliging. De Berlin Group, een Europees initiatief op het gebied van standaardisatie en harmonisatie van betalingsverkeer, heeft hiertoe al stappen gezet met het European Standards-initiatief, met als doel standaardisering van api's voor PSD2-compliance. Daarbij zijn beveiligingsstandaarden cruciaal. Deze worden daarom samen met de bankensector ontwikkeld.

5.

Verdere toename gebruik machine-learning

De inzet van machine-learning, of het herkennen van afwijkende patronen in netwerkverkeer en computerprocessen, is al in gang gezet. Echter, gezien de toenemende dreiging zal dit zich alleen maar verder ontwikkelen. Er zijn al meerdere oplossingen die machine-learning inzetten, zoals bijvoorbeeld DarkTrace en IBM Watson. Deze oplossingen leren wat de 'normale' gedraging van een systeem is en waarschuwen bij afwijkende patronen. Overigens is de meest effectieve oplossing vaak de combinatie van machine-learning met een goed getrainde analist.

6.

Distributed storage en computing

Een van de drie doelen van cybersecurity is er zorg voor dragen dat toegang tot systemen en netwerken gewaarborgd is. In een traditionele beveiligingsaanpak gaat het dan om business-continuitymanagement van systemen en datacenters. Maar nu kan dat ook anders met gedistribueerde opslag en rekenkracht. De introductie van nieuwe toepassingen zoals 'fog computing' is veelbelovend. Hierbij wordt het verwerken en de opslag van gegevens buiten de organisatie geplaatst, maar wel relatief dicht bij waar het nodig is.
Pioniers op dit terrein zie je bijvoorbeeld in SOMN, een startup die de ethereum blockchain benut om gedistribueerde rekenkracht aan te bieden. Of STORJ, een startup die decentrale opslag aanbiedt bij derden, beveiligd met blockchaintechnologie. Sterke encryptie en distributie van data over meerdere nodes minimaliseren het risico van een single point of failure. In 2018 voorziet INNOPAY meer applicaties die security-by-designtechnologie benutten.

DE INTRODUCTIE VAN NIEUWE TOEPASSINGEN ZOALS FOG COMPUTING IS VEELBELOVEND

7.

Cybersecurity platformation

Platformation is een ontwikkeling om in de gaten te houden. We zien in toenemende mate platforms waar zelfstandige securityresearchers en ethical hackers ingehuurd kunnen worden. Synack is daar een aardig voorbeeld van. Dit is een platform waarop (gescreende) cybersecurityspecialisten zich aanbieden, en die organisaties ondersteunen bij penetration testing en white hat hacking.

8.

Security rating agencies en achtergrondchecks

Het technologische ecosysteem fragmenteert. Het aantal IT-aanbieders neemt toe en organisaties lopen het risico dat zij het overzicht kwijtraken, terwijl het management onder voortdurende tijdsdruk beslissingen moet nemen. Beveiligingslekken liggen op de loer als meerdere partijen niet van elkaar weten wie wat precies doet. De ketting is zo sterk als de zwakste schakel.
Organisaties moeten in kaart brengen of de beveiliging, zowel van zichzelf als van bestaande en toekomstige partners, voldoet. Immers, het heeft weinig zin om volop te investeren in eigen beveiliging als een partner de zaken niet op orde heeft.
Net als bij creditchecks zien wij dat in 2018 marktdata nodig is om beveiliging goed op waarde te schatten. Momenteel zijn er al spelers actief op dit specifieke gebied, bijvoorbeeld Bitsight en Checkr. Het aantal beveiligingsbenchmark-aanbieders zal zeker toenemen.

Dit waren ze dan. Acht trends met kansen en bedreigingen. Deze trends kunnen (of zullen) in 2018 een rol spelen in de cybersecuritystrategie. ✖

Dr. Rob van der Staaij CISSP CCSP CISA CISM CRISC CEH CPT is principal Cybersecurity bij INNOPAY, consultancybureau gespecialiseerd in digitale transactions, en spreker en docent op het gebied van cybercrime & cybersecurity.

Drs. Jelger Groenland CISSP is senior manager Cybersecurity en Practice Lead bij INNOPAY. Hij heeft 14 jaar ervaring en adviseert senior management en c-level-executives op het gebied van cybersecurity.