TD SYNNEX

**Security Solutions**

# Lastige securityvragen?

## Met onze antwoorden kun je de hele wereld aan

**ICT-security is een complex domein dat veel vraagtekens oproept. Om je te helpen, zetten wij hieronder enkele veelvoorkomende vragen op een rij. Staat je vraag er niet bij? Neem dan gerust contact met ons op. Wij helpen je graag.**

### 1. Wat is Cybersecurity?

Cybersecurity is de verzamelnaam voor alle diensten en oplossingen die de ICT beschermen tegen dreigingen van buiten. Dat gaat veel verder dan bescherming tegen malware. Denk aan het tegenhouden van hackers, versleuteling van bestanden zodat onbevoegden deze niet kunnen lezen en maatregelen voor gegevensherstel.

### 2. Waarom is cybersecurity nodig?

Een cyberaanval kan leiden tot grote financiële schade en zelfs faillissement. Denk aan de inkomsten die je klant misloopt en het verlies aan productiviteit als ICT-systemen niet beschikbaar zijn door een cyberaanval. Of aan cybercriminelen die een organisatie dwingen of verleiden tot het betalen van grote sommen geld. Na een aanval heeft de organisatie mogelijk ook nog te maken met kosten voor het herstel van ICT systemen en van het imago. Dit zijn risico's die je met cybersecurity beperkt.

### 3. Wat zijn nu de grootste dreigingen?

Enkele ernstige cyberdreigingen zijn:

#### Ransomware

Dit is malware die de bestanden op een getroffen systeem onleesbaar maakt voor de eigenaar. Het slachtoffer wordt geconfronteerd met een keuze: losgeld betalen in de hoop weer toegang te krijgen tot de data, of de bestanden voor altijd kwijt zijn. Ransomware is voor criminelen buitengewoon lucratief. Het is daardoor een van de meest voorkomende én schadelijke vormen van cybercrime.

#### Cryptojacking

Een cyberdreiging die aan populariteit wint is cryptojacking. Hierbij installeren de criminelen in het geniep een programma op het systeem van anderen dat cryptomunten delft. Zo verdienen ze aan de rekenkracht van het systeem van het slachtoffer, dat te maken krijgt met tragere servers en clients.

### Phishing

Cybercriminelen sturen emails die afkomstig lijken van een betrouwbare organisatie. Zo proberen ze hun slachtoffer op een link te laten klikken of een kwaadaardig bestand te laten openen. Het doel is om informatie zoals wachtwoorden buit te maken, of om malware te installeren. Zeer gerichte aanvallen op een specifieke organisatie of persoon worden spearphishing genoemd.

### Distributed Denial of Service (DDoS)

Hierbij bestookt de crimineel de website van het slachtoffer met gigantische hoeveelheden internetverkeer. Dit is zo overweldigend dat de hele omgeving plat komt te liggen. Dit kan soms dagenlang aanhouden.

### Computerinbraak

Dit is een klassieke vorm van computercriminaliteit waarbij de hacker een systeem binnendringt.
Op deze manier kan hij data stelen, malware installeren of het systeem onklaar maken.

## 4. Ik ben getroffen door ransomware. Moet ik betalen?

Geregeld duiken in de media berichten op dat een prominente organisatie cybercriminelen heeft betaald om van ransomware af te komen. Dit is echter bijzonder riskant, en niet alleen omdat het crimineel gedrag beloont. Het is om te beginnen onzeker of de criminelen hun belofte wel nakomen en een werkende sleutel geven. Het is ook mogelijk dat ze een achterdeur in de omgeving openzetten, zodat ze in de toekomst opnieuw kunnen toeslaan.

Maar wat als jouw klant echt met de rug tegen de muur staat? In zeldzame gevallen hebben securitybedrijven de decryptieserver van de criminelen gekraakt en kunnen ze data weer ontcijferen. Heeft je klant dat geluk niet, dan is de beste optie om de systemen schoon te vegen en de backups terug te zetten.
De data waar geen backup van is, moet helaas als verloren worden beschouwd.

## 5. Wat moet ik beveiligen?

Helaas geldt voor ICT security de aloude typering dat het zo sterk is als de zwakste schakel. Security moet dus op alle niveaus van de infrastructuur aangebracht worden. Van het netwerk en de routers tot aan de servers en de desktops. Steeds vaker geldt dit ook voor mobiele apparaten en apparaten aangesloten op het Internet of Things (IoT).

## 6. Welke soorten beveiliging zijn er?

Enkele voorbeelden van securitymiddelen zijn:

### Firewall

Een securityoplossing die ongeautoriseerde netwerkverbindingen in de gaten houdt en netwerkverkeer op basis van regels doorlaat of stopt.

### Endpointsecurity

Endpoints zijn apparaten als smartphones, desktops, laptops, tablets en kiosken. Endpointsecurity is de kunst van het beveiligen van deze apparaten. Dat kan door een stuk software op de apparaten zelf te installeren, of door ze in de gaten te houden via een externe server.

### E-mailsecurity

Dit zijn de oplossingen specifiek gericht op het beveiligen van de emailomgeving. Onderdelen zijn bijvoorbeeld spamfilters, mailscanners en antiphishing.

### Back-up en recovery

Het veiligstellen van data door deze regelmatig naar een externe locatie weg te schrijven. Mochten er data verloren gaan, dan zijn deze vanaf backup terug te zetten. Door de opkomst van ransomware zijn backup en recovery alleen maar belangrijker geworden.

### Anti-DDoS

Oplossingen die de online dienstverlening beschermen tegen Distributed Denial of Serviceaanvallen.

Er zijn meerdere manieren om een DDoS-aanval af te slaan.

Een mogelijkheid is om het netwerkverkeer door een speciale ‘wasstraat’ te laten lopen waar de echte aanvragen worden gescheiden van het kunstmatige verkeer. Dit minimaliseert de hinder die echte bezoekers ondervinden van de aanval.

### Identity en Access Management (IAM)

Deze oplossingen regelen de toegang van gebruikers tot applicaties en ICTsystemen. Niet alleen om onbevoegden buiten te houden, maar ook zodat medewerkers niet constant opnieuw hun wachtwoord in hoeven te voeren of tientallen wachtwoorden moeten onthouden.

## 7. Dus ik moet dat allemaal gaan afnemen?

Perfecte beveiliging is helaas onmogelijk. Ja, het is cruciaal om op ieder niveau aan security te doen. Maar gezien de kosten is het belangrijk keuzes te maken en prioriteiten te stellen. Dat kan bijvoorbeeld door de volgende vragen te stellen aan je klant:

- Welke data en systemen zijn cruciaal voor de bedrijfsvoering?
- Welke dreigingen hebben de grootste impact op het bedrijf?
- Waar in de ICT zitten de zwakheden en hoe lost de organisatie die op?
- Wat kan je klant doen als het alsnog misgaat?

Het is zeer belangrijk om deze vragen om de zoveel tijd opnieuw te beantwoorden.

Bedrijven veranderen, en dreigingen ook. Om er echt werk van te maken, is een risicoanalyse nodig.

### 8. Hoe maak ik een risicoanalyse?

Voor je security kunt toepassen, moet je eerst weten waar de risico's bij je klant liggen en hoe deze aan te pakken. Daarvoor is een risicoanalyse nodig. De precieze vorm hangt af van de specifieke organisatie en ICT omgeving. Maar de analyse bestaat ruwweg uit vier stappen en bijbehorende vragen:

- Identificatie. Welke onderdelen van de infrastructuur zijn absoluut kritisch voor het bedrijf, waar staan de gevoelige data en hoe worden deze verstuurd? Maak voor ieder onderdeel een risicoprofiel aan waarin staat wat eventueel mis kan gaan, en hoe ernstig de schade kan zijn.
- Assessment. Wat moet er per onderdeel gebeuren om het risico te verlagen, en hoeveel tijd en geld is hiervoor beschikbaar? Hierin moet je de samenhang meenemen tussen de middelen, dreigingen, kwetsbaarheden en eventuele beveiligingsmaatregelen.
- Maatregelen. Welke maatregelen kies je uiteindelijk om de risico's te verlagen? Deze keuze maak je als de prioriteiten zijn gesteld en duidelijk is hoeveel budget en mankracht beschikbaar is.
- Implementatie. Wanneer en hoe implementeer je de maatregelen? Hier teken je het concrete implementatietraject van de gekozen maatregelen uit.
-

Dit geeft nog een mogelijkheid om het budget aan te passen en accenten te verleggen.

### 9. Zijn bepaalde platformen kwetsbaarder dan andere?

Ja, maar niet altijd omdat de producenten er onvoldoende aandacht aan besteden. Veelgebruikte platformen zijn interessanter voor cybercriminelen, omdat ze via deze platformen meer slachtoffers kunnen maken. Ook belangrijk is de ondersteuning van leveranciers. Platformen die geen updates meer krijgen, zijn vanzelfsprekend kwetsbaarder voor aanvallen dan actief ondersteunde platformen.

### 10. Is Cloudcomputing veilig?

Cloudcomputing is niet veiliger of onveiliger dan traditionele ICT. Veel hangt af van hoe serieus de cloudprovider met security omgaat, en in hoeverre de klant zijn eigen verantwoordelijkheid neemt als het gaat om het beveiligen van data die in de cloud staat. Maar cloudproviders hebben zeker de laatste jaren veel gedaan aan hun security, omdat hun klanten hier zeer dringend om vragen.

### 11. Waar zit het allergrootste risico?

Niet in de techniek, want aan vrijwel iedere geslaagde cyberaanval gaat een menselijke fout vooraf. Hoe geloofwaardig een mailtje ook overkomt, meestal heeft de gebruiker die op de kwaadaardige link klikte enkele overduidelijke signalen over het hoofd gezien. Of de beheerder is een patch vergeten te installeren. Of iemand negeerde een waarschuwing op het scherm.

Techniek is voorspelbaar, menselijk gedrag is dat echter niet. Dat maakt de gebruiker het allergrootste risico.

### 12. Hoe maak ik mijn mensen securitybewust?

Gezond verstand is natuurlijk een belangrijk gegeven, maar je kunt niet van medewerkers verwachten dat ze alles weten en altijd scherp zijn. Trainingen en opfriscursussen helpen enorm, net als duidelijk beleid.

Ook zijn er oplossingen beschikbaar die medewerkers tijdens hun werk scherp houden. Denk aan vragen die de gebruiker na het klikken op een link krijgt voorgelegd. 'Waarom vertrouw je deze link?' of 'Komt de mail van iemand die je kent?' zijn mogelijke vragen waarmee ICT werknemers kan confronteren. Wel met mate, want geïrriteerde medewerkers zijn onvoorzichtige medewerkers.

### 13. Welke beveiliging is voor alle organisaties verplicht?

Wet en regelgeving schrijft niet zozeer voor hoe een organisatie zijn ICT moet beschermen, maar wat ze moeten beveiligen. Zo schrijft de Algemene verordening gegevensbescherming (AVG) van de Europese Unie voor dat persoonsgegevens beveiligd moeten worden, en dat organisaties die beveiliging ook moeten kunnen aantonen. Mocht het toch misgaan, dan moeten bedrijven dit melden bij de privacytoezichthouder, en bovendien laten zien dat ze alles hebben gedaan om herhaling te voorkomen.

### 14. Heeft security impact op de prestaties van mijn ICT?

Hoewel dat afhangt van het soort security, zijn de tijden van virusscans die alle rekenkracht opeten onderhand wel voorbij. Het blijft echter een kwestie van goed instellen. Overdreven regels kunnen legitieme applicaties tegenhouden en gebruikers onterecht buitensluiten. Een backupoplossing die iedere minuut data over het netwerk pompt, is ook niet bevorderlijk voor de prestaties.

### 15. Hoe weet ik waar ik nu sta?

Er zijn verschillende manieren om de ICT-security te testen. Enkele daarvan zijn:

- **Penetratietesten**
  Hierbij probeert een gecertificeerde hacker de omgeving in opdracht actief binnen te dringen. Daarvoor gebruiken ze verschillende methodes die cybercriminelen ook aanwenden. Na afloop stelt hij of zij een rapport op met de resultaten en advies. De resultaten kunnen zeer confronterend zijn.

- **Securityscans**
  Een securityscan is veel minder ingrijpend dan een penetratietest. Hierbij voert de specialist alleen enkele routinetests uit om mogelijke kwetsbaarheden te vinden. Denk aan het geautomatiseerd uitproberen van standaardwachtwoorden of het scannen naar openstaande poorten. Omdat het minder ingrijpend is, kan een securityscan vaker worden uitgevoerd. Eens per kwartaal is het algemene advies.

- **Phishingtests**
  Bij phishingtests richten de securityspecialisten zich op de werknemers. Ze sturen dan een phishingmail rond en kijken welke medewerkers op de link in de mail klikken. Dit geeft een beeld van hoe bewust de medewerkers zijn en hoeveel risico ze nemen. Phishingtests kunnen ook deel uitmaken van een penetratietest.

### 16. Welke technische basismaatregelen kan ik hoe dan ook nemen?

Security is nooit een kwestie van technologie alleen. Vrijwel alle securityincidenten beginnen bij een menselijke fout. Denk aan medewerkers die op een link klikken of een gevonden USB-stick in hun pc steken. Interne bewustwording is hoe dan ook een eerste stap die ieder bedrijf kan nemen. Een ander belangrijk punt is dat de meeste cyberaanvallen gebruikmaken van kwetsbaarheden waarvoor allang een patch bestaat. Patchhygiëne is, net als bewustwording, iets dat iedere organisatie op weg helpt. En ieder bedrijf moet op zijn minst voorbereid zijn op het ergste. Een geslaagde aanval waarbij alle data verdwijnen, is voor iedereen funest. Dit onderstreept het belang van goede backups. Deze beperken op zijn minst de schade.

### 17.Moet ik zelf securityspecialisten aannemen?

Dat is een mogelijkheid voor wie het budget heeft, maar voor de meeste bedrijven is dit onhaalbaar. Security is bovendien geen ‘catchall’ categorie waarbij een securityspecialist echt alle facetten goed onder de knie heeft. Een expert op het gebied van encryptie is niet altijd helemaal op de hoogte van malwarebestrijding, bijvoorbeeld. Je klant kan niet verwachten dat één persoon de hele omgeving goed beveiligt. Voor zover zo iemand al bestaat, zal de marktwaarde astronomisch zijn. De securitybehoefte is niet altijd groot genoeg om dat te verantwoorden.

Een goed alternatief is het uitbesteden van security aan gespecialiseerde bedrijven. In de praktijk deelt je klant de expertise dan met anderen, evenals de kosten.

### 18. Hoe kies ik een leverancier voor security?

Hier zijn meerdere overwegingen voor, waaronder:

- Wil je klant een one-stop-shop, waar de hele beveiliging door wordt uitgevoerd? Of wenst hij of zij voor ieder beveiligingsdomein een gespecialiseerde leverancier?
- Kun je de beveiliging van de data uitbesteden, of mogen externen er absoluut geen toegang toe hebben?
- Wil je klant een partij die software implementeert en hooguit een bemande helpdesk heeft, of eentje die de omgeving 24/7 in de gaten houdt?

### 19. Wat moet ik doen als het alsnog mis gaat?

Twee dingen genieten de absolute prioriteit: schadebeperking, gevolgd door het voorkomen van herhaling. Onder schadebeperking vallen handelingen als het snel reageren en het eventueel terugzetten van backups, maar bijvoorbeeld ook het voldoen aan de wettelijke eisen als het gaat om het melden van een datalek, zoals voorgeschreven in de Algemene verordening gegevensbescherming. Hieronder vallen ook de te nemen handelingen om herhaling te voorkomen. Van het uitvoeren van de benodigde patches en het dichten van lekken tot het aanpassen van het beleid.

### 20. Hoe zorg ik voor een continue verbetering van mijn security?

ICT beveiliging is nooit 'af': de beveiliging kan nooit perfect zijn, maar verbetering is altijd mogelijk. Om tot een continue verbetering te komen, is een gestructureerde aanpak nodig. Dat houdt in dat jouw klant constant dezelfde gedachtenvolgorde aanhoudt. Een voorbeeld dat hij kan aanhouden is het PDCA-model:

1. Plan ('Wat moet er gebeuren?')
2. Do ('Dat doen we nu!')
3. Check ('Werkt alles nu?') en
4. Act ('Nee, we moeten hier nog iets wijzigen').

En daarna begint de cyclus weer opnieuw.

### 21. Wat levert een goede security mij op?

Het is een misverstand te denken dat cybersecurity niet meer is dan een verzekeringspolis. Security heeft ook tastbare voordelen voor bedrijven, waaronder: Vertrouwen van klanten – Klanten die zien dat hun dienstverlener zijn cyberveiligheid goed op orde heeft, zullen dit zien als een teken van betrouwbaarheid en professionaliteit.

- Hogere uptime – Minder verstoringen betekent meer business. En goede cybersecurity vermindert het aantal verstoringen van de ICTomgeving.

- Een basis voor nieuwe diensten – Een goed beveiligde omgeving stelt jouw klant in staat om meer garanties te kunnen bieden, ook voor op het oog riskantere diensten.

- Betrouwbare data – Doordat de integriteit van de data beter is gezekerd, is er meer data waar beslissingen op kunnen worden genomen.

### 22. Kan ik me ook verzekeren tegen de schade van cybercrime?

Over verzekeringen gesproken: steeds meer verzekeraars bieden inderdaad een polis die de schade veroorzaakt door cybercrime dekt. Hoe beter de beveiliging bij jouw klant is ingeregeld, des te lager de kosten voor de verzekering.

TD SYNNEX

### 22. Hoe blijf ik up-to-date van de nieuwste cyberdreigingen?

Het dreigingslandschap verandert continu, met nieuwe aanvallen, maar ook nieuwe manieren om de omgeving te beschermen. Partijen die je klant hiervan op de hoogte kunnen houden, zijn onder meer:

- De ICTpartners, vooral partners die zich specialiseren in security
- Het Nationaal Cyber Security Centrum en het Digital Trust Center van de overheid
- Leveranciers van antivirusoplossingen

## Geïnteresseerd in wat we voor jouw security business kunnen bereiken?

Neem contact op via:

**tdsecurity.nl@tdsynnex.com**

of kijk voor meer info op de website:

**https://connect.tdsynnex.nl/solutions/security**