QS solutions

Whitepaper

Security Assessment: de eerste stap in cyberveiligheid

Breng je cybersecurity volwassenheid in kaart met een periodiek assessment, en ontdek waar de kwetsbaarheden en risico's liggen. Zo bescherm je je organisatie gericht en efficiënt tegen cyberaanvallen.

Content

1. De cyberrisico’s van het nieuwe normaal

2. Cyberbestendig worden

3. CSAT in een notendop

4. Vinger aan de pols houden

De cyberrisico’s van het nieuwe normaal

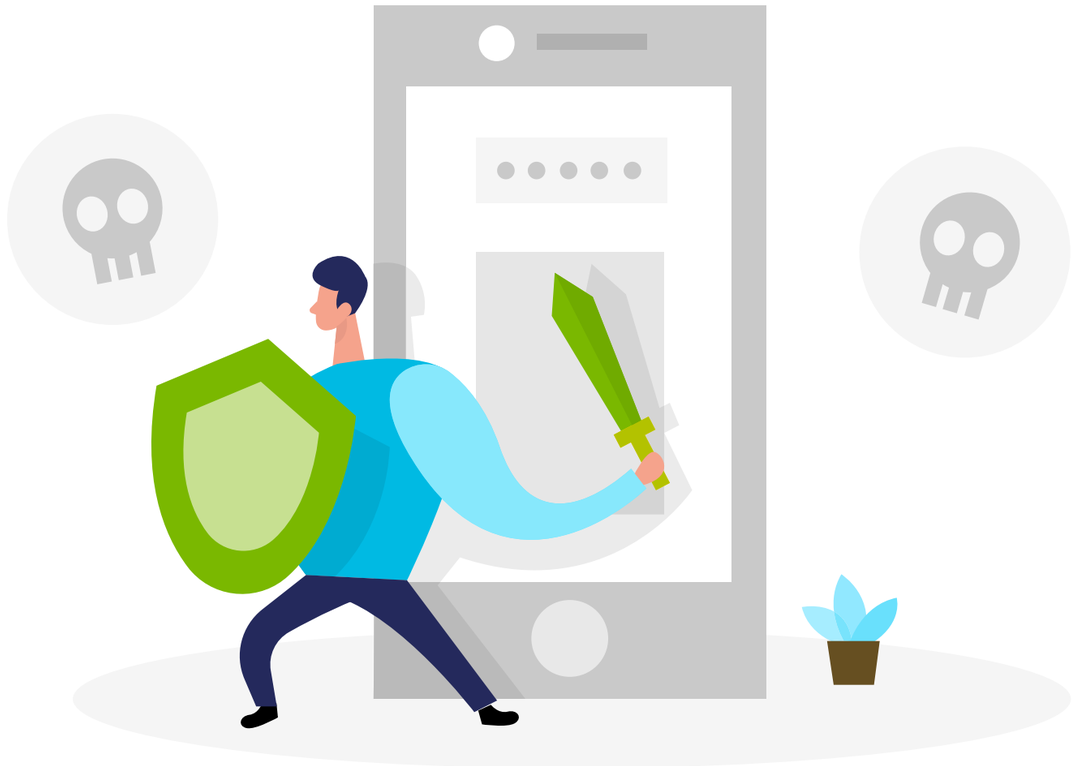
De coronapandemie zette ook onze digitale wereld op z’n kop. Terwijl het virus zich in rap tempo over de wereld verspreidde en zorgde voor chaos, onzekerheid en verwarring, ontstond een digitaal walhalla voor cybercriminelen. Thuiswerken werd de norm voor miljoenen mensen, ook in branches waar dit vóór de pandemie nog zeker niet de gewoonte was. Deze manier van werken raakte in een stroomversnelling, waardoor de al aanwezige cyberrisico’s nog groter en zichtbaarder werden. Vaak werd gewerkt met een suboptimaal beveiligde infrastructuur en namen medewerkers hun toevlucht tot privé-apparatuur en moderne apps om met collega’s en klanten te communiceren, vaak zonder toestemming van de IT-afdeling.

Ondertussen werden hackers opportunistisch en gingen steeds slimmer, meer geavanceerd en beter georganiseerd werken. En dat zien we terug in de cijfers. Volgens een rapport van Interpol [1)] heeft de pandemie ongekende gevolgen gehad voor het wereldwijde cyberdreigingslandschap, en de verwachting is dat het naar alle waarschijnlijkheid zal blijven verslechteren. Cybercriminelen ontwikkelen en voeren hun aanvallen in een alarmerend tempo uit. Ze maken hierbij gebruik van de angst en onzekerheid die worden veroorzaakt door de onstabiele sociale en economische situatie over de hele wereld. Tegelijkertijd groeit de kans op cyberinbraken en -aanvallen door de toenemende afhankelijkheid van connectiviteit en de digitale infrastructuur.

Ga maar na: hoeveel technologie heeft jouw organisatie allemaal nodig om up and running te blijven? Elke applicatie en elk apparaat is een risico. En door het massale thuiswerken heb je veel minder onder controle welke applicaties en apparaten je medewerkers gebruiken.

Het is dus niet meer de vraag óf, maar wanneer jouw organisatie te maken krijgt met een beveiligingsbreuk.

1) Interpol – Cybercrime: COVID-19 Impact (augustus 2020)



Schade

En als het misgaat, kan dit enorme gevolgen hebben. Niet alleen op financieel vlak – denk bijvoorbeeld aan het betalen van losgeld en de kosten die gepaard gaan met downtime, het verlies van data en het herstellen van systemen – maar ook zeker met het oog op de reputatie van je bedrijf en het vertrouwen van de klant.

Het feit dat datalekken steeds vaker voorkomen en bovendien breed worden uitgemeten in de media, betekent dat klanten zich bewuster zijn dan ooit dat dataveiligheid geen vanzelfsprekendheid (meer) is. Zij laten dit steeds vaker meewegen in hun keuze voor een bedrijf of organisatie. Volgens onderzoek2) is zelfs *84% van klanten loyaler naar bedrijven met een strenge databeveiliging*.

Ook vanuit de EU wordt inmiddels regelgeving opgesteld rondom verplichte cyberbeveiliging. De nieuwe regels gaan niet alleen gelden voor vitale bedrijven en instellingen zoals banken, ziekenhuizen, zorginstellingen en nutsbedrijven. Ook andere bedrijven met een jaaromzet van (ten minste) 10 miljoen euro en vijftig werknemers zijn straks verplicht om hun IT-systemen na te lopen op kwetsbaarheden, risicoanalyses uit te voeren, hun beveiliging te verbeteren en liefst dagelijks back-ups te maken.

Steeds meer directieleden en managementteams beseffen inmiddels dat beveiliging niet *slechts een technologisch vraagstuk is*. Het is een opgave voor de hele organisatie en vraagt om visie vanuit de boardroom. Cybersecurity is dus een vitaal onderdeel geworden van de organisatiestrategie, al wordt dat nog regelmatig vergeten.

2) ZDNet: Top 8 trends shaping digital transformation in 2021

Cyberbestendig worden

Als organisatie gaat het er dus om dat je cyberbestendig moet worden: je moet cyberaanvallen kunnen overleven, kritieke processen en activiteiten kunnen handhaven en nieuwe technologieën kunnen omarmen. De continu veranderende dreigingen vergen ook een duidelijke wendbaarheid. Je moet kunnen meebewegen met wat er gebeurt, maar wel vanuit een heldere visie. En met een doordachte, strategische aanpak van informatiebeveiliging met uitgekiende processen, waardoor je je kritieke processen en activiteiten blijft beschermen, altijd alert blijft en snel en veerkrachtig reageert op incidenten.

En dat alles zonder de productiviteit van de organisatie te raken. Vooral dat laatste is belangrijk, want je medewerkers *moeten* natuurlijk toegang blijven houden tot de applicaties en data waarmee ze hun werk kunnen uitvoeren, ongeacht of ze op kantoor zijn, vanuit huis werken of onderweg zijn. Dat is dé uitdaging voor security op dit moment.

Een goed begin...

Waar begint dan die cyberbestendigheid? En hoe kom je tot een sterke beveiligingsstrategie? Feit is dat een traditionele databeveiliging niet meer volstaat. Een veilig en compliant netwerk on-site inrichten voor je organisatie, en proberen daar alle bedrijfsmiddelen onder te brengen, is niet meer van deze tijd. In dit digitale tijdperk is een bredere, maar bovenal ook adaptieve strategie nodig. Eentje die zich kan aanpassen aan de toenemende complexiteit en dynamiek van onze manier van werken. Die er rekening mee houdt dat medewerkers altijd en overal moeten kunnen werken, vanuit ieder apparaat. Het enige dat ze hoeven te doen, is inloggen op hun digitale werkplek. Dat brengt andere risico's met zich mee en vereist een herziende cybersecuritystrategie.

Een logische – en noodzakelijke – eerste vraag is: hoe gaat jouw organisatie *op dit moment* om met digitale dreigingen? Hoe volwassen zijn jouw huidige cybersecuritymaatregelen? En kun je proactief handelen wanneer dat nodig is? Maar vooral: waar moet je beginnen met het herzien van de securitystrategie? Waar liggen de kwetsbaarheden en risico's?

Voor de meeste bedrijven en organisaties is het simpelweg niet haalbaar om meerdere grote wijzigingen in één keer te realiseren. Klein beginnen is dan ook het devies. Een gefaseerde aanpak, waarin je je eerst richt op de gebieden waar de cybersecurity nog onvoldoende volwassen is. Die gebieden worden mede bepaald op basis van de beschikbare resources en prioriteiten. Welk budget is beschikbaar? Wat zijn de directe zakelijke behoeften? Oftewel: wat moet je nú aanpakken en wat is mogelijk?

Nulmeting

Om effectief te kunnen starten met het aanpakken van de securitystrategie is het dus belangrijk om *het beginpunt* te bepalen, een nulmeting te doen. Hoe volwassen is jouw cybersecurity nu? Hoe groot is de reikwijdte van je informatiebeveiliging? De volgende elementen geven daarvoor een sterke indicatie:

- Hoe sterk is de **authenticatie**? Gebruik je een sterke Multi Factor Authenticatie? Hoe minimaliseer je het risico van identiteitsinbreuk?

- Hoe adaptief is jouw **toegangsbeleid**? Hanteer je heldere beleidsregels voor acceptabele toegang voor resources? En hoe dwing je die af?

- Maak jij al werk van **microsegmentatie**? In hoeverre is jouw organisatie op weg naar een allesomvattende en gedistribueerde segmentatie met behulp van softwarematig gedefinieerde microperimeters?

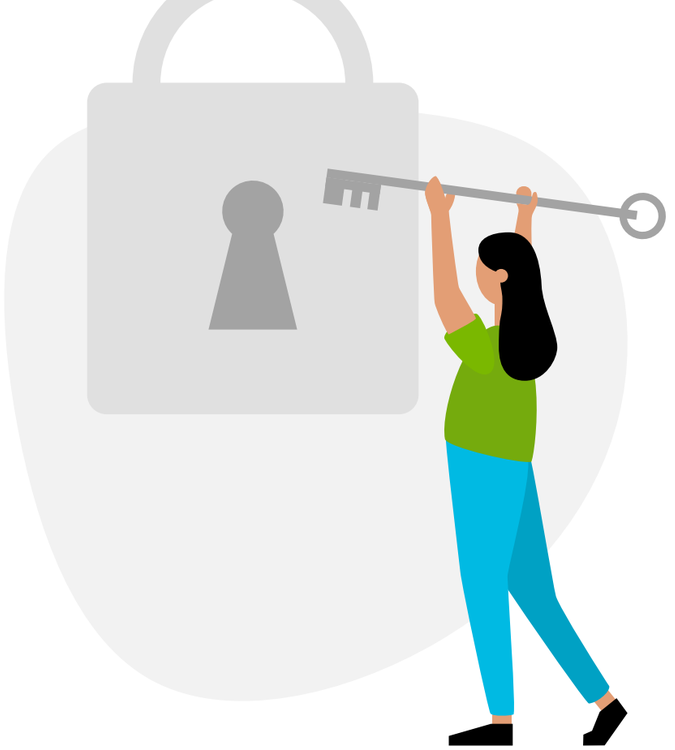
- Werk je al met **geautomatiseerde waarschuwingen en herstelacties** om de gemiddelde tijd tussen aanval en reactie te minimaliseren?

- Gebruik je al **kunstmatige intelligentie en cloud-intelligence** om in real-time afwijkingen te detecteren en hierop te reageren?

- In hoeverre **classificeer en bescherm** jij je data? Hoe minimaliseer je gevoelige data tegen blootstelling aan schadelijke of onbedoelde exfiltratie, oftewel het ongeautoriseerd vrijgeven van gegevens uit computersystemen?

Van hieruit kun je vervolgens bouwen aan de cyberweerbaarheid van de organisatie.

Om gestructureerd en gedetailleerd inzicht te krijgen in de mate van volwassenheid van je cybersecurity op alle relevante elementen, adviseren we bij QS solutions een **cybersecurity assessment**. Dit onderzoekt je hele bedrijfsnetwerk en je Microsoft 365- en Azure-omgeving op mogelijke kwetsbaarheden, en geeft hiermee een helder overzicht van kwetsbaarheden en risico's.



CSAT in een notendop

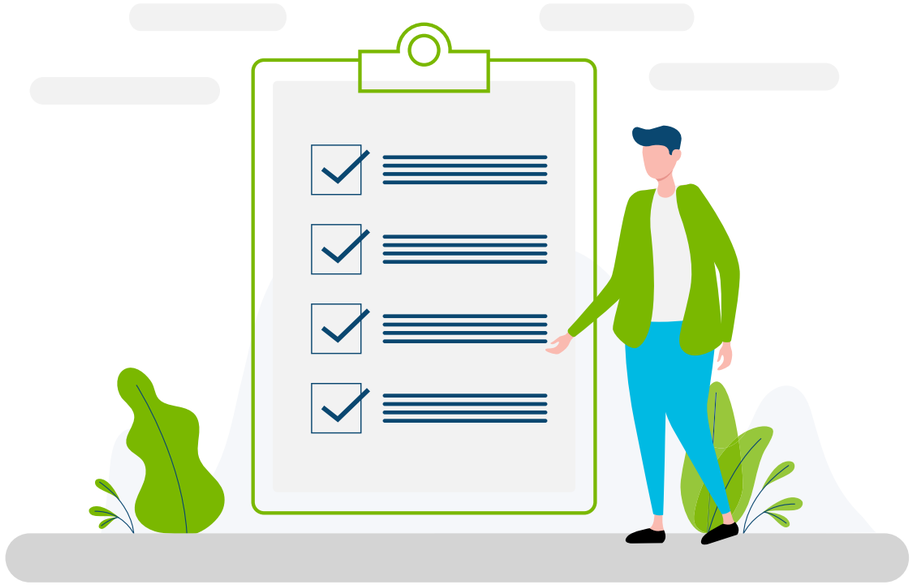
Onze Cyber Security Assessment Tool (CSAT) is gebaseerd op het CIS-framework, een veelgebruikte set van best practices die is ontworpen voor het gestructureerd beheren van cyberrisico's binnen bedrijven en organisaties. Het helpt je om kritische vragen over het cyberbeveiligingsprogramma van jouw organisatie te beantwoorden, zoals welke inventaris je moet beschermen en waar hiaten in de beveiliging liggen.

Het security assessment biedt de volgende features:

- On premise – de assessment tool wordt geïnstalleerd op een server in het netwerk
- Endpoints – door middel van een steekproef worden de laptops, desktops en servers in het netwerk gecheckt
- Microsoft 365 – controle op alle gebruikte (en gedeelde) diensten
- Azure-platform – inzicht in veilig gebruik van het cloudplatform
- (Azure) Active Directory – evaluatie van de volledige (Azure) Active Directory-omgeving
- Enquête – een van onze security consultants vraagt naar securityprocessen en -procedures

Als onderdeel van het security assessment kijken we onder andere of Windows veilig is geconfigureerd en of de juiste patches zijn doorgevoerd. Ook controleren we administratieve permissies en externe gebruikers in Microsoft 365, Teams of de gedeelde documenten in SharePoint. Deze inzichten bepalen de huidige securityvolwassenheid van de organisatie, op basis waarvan concrete verbeteracties kunnen worden voorgesteld.

Het assessment past naadloos in een Zero Trust-beleid waarin alle medewerkers, apparaten en applicaties worden beveiligd, waar die zich ook bevinden, zonder dat dit een belemmering vormt voor de productiviteit. Hoe zo'n 'Zero Trust'-beleid wordt ingevuld verschilt per organisatie, maar de basis is hetzelfde, namelijk het veiligstellen van bedrijfsgegevens en -applicaties op basis van het 'vertrouw nooit, controleer altijd'-principe. Vanuit deze visie richt je je op de beveiliging en compliance van bedrijfsmiddelen, ongeacht hun fysieke locatie of plaats in het netwerk.



Gericht verbeteren

Dankzij het security assessment krijg je in korte tijd inzicht in welke cyberrisico's er zijn voor jouw organisatie en in hoeverre de huidige securitymaatregelen voldoende bescherming bieden. Het legt potentiële kwetsbaarheden en risico's bloot, waardoor je geïnformeerde besluiten kunt nemen over prioriteiten binnen je cybersecurity: hier gaan we eerst ons securitybudget aan besteden.

De CSAT biedt een helder plan van aanpak om de cyberveiligheid van je organisatie te verbeteren, precies waar dat nodig is. En inclusief duidelijke technologische en procedurele maatregelen, zodat je meteen aan de slag kunt en je middelen doelgericht inzet.

Met een cybersecurity assessment krijg je inzicht in de securityrisico's van de organisatie en prioriteer je snel en effectief de voorgestelde verbeteracties op basis van feiten.

Vinger aan de pols houden

Na het doorvoeren van de verbeteracties is het belangrijk om door middel van een tweede assessment te meten wat er is verbeterd ten opzichte van de nulmeting. Vergeet niet het management team te betrekken in de presentatie van de resultaten, zodat ook zij op de hoogte zijn van de verminderde risico's en de toegenomen cybervolwassenheid van de organisatie.

De volgende stap is het prioriteren, uitwerken en plannen van de volgende doelstellingen. Cybersecurity heeft nu eenmaal geen begin- en eindpunt. Het is onmogelijk om alles in één keer goed te doen en daarom is het belangrijk om er een doorlopend aandachtspunt van te maken.

Zorg doorlopend voor een nauwkeurige documentatie van de status, voortgang en verbeteracties. Dit is niet alleen waardevol voor intern gebruik, maar ook onmisbaar met het oog op de naleving van wet- en regelgeving, bijvoorbeeld omtrent GDPR/AVG.

De IT-wereld verandert in een rap tempo, en dat geldt ook voor cybercriminelen. Digitale bedreigingen evolueren voortdurend. Ook al biedt een eenmalig assessment een gedetailleerde nulmeting van de huidige cybervolwassenheid en de mogelijke kwetsbaarheden en risico's, het neemt niet weg dat het van cruciaal belang is om vinger aan de pols *te blijven* houden en voortdurend alert te blijven.

Leun daarom niet achterover, maar blijf proactief de securitystatus evalueren en de voortgang rapporteren. Het **periodiek herhalen van het security assessment** is een essentieel onderdeel van een gezonde securitystrategie. Het geeft een beeld van de ontwikkeling in de cyberbestendigheid van de organisatie als geheel en van de verschillende onderdelen van de infrastructuur.

Zo kun je uiteenlopende beveiligingsrisico's beheersen en blijf je nieuwe vormen van cybercrime voor, zónder dat de informatiebeveiliging de productiviteit belemmert.

Over QS solutions

Bij QS solutions weten we hoe kwetsbaar organisaties zijn. Én welke gevolgen het kan hebben als een organisatie niet proactief de cybersecurity volwassenheid verbetert. We starten met onze **Cyber Security Assessment Tool (CSAT)** om snel en eenvoudig de status van de beveiliging in beeld te brengen.

Op basis daarvan kunnen we gericht de grootste risico's aanpakken. Bijvoorbeeld met de cloudnative beveiligingsoplossingen van Microsoft. Omdat je met het Microsoft platform de uiteenlopende beveiligingsrisico's beheerst en zorgt dat eindgebruikers altijd productief en veilig blijven werken.

Met een periodiek assessment blijf je bovendien altijd op de hoogte van de cyberrisico's binnen de organisatie en weet je feilloos welke mogelijke kwetsbaarheden je dringend moet aanpakken. Dé manier om op basis van feiten een actieplan te definiëren.

Wil je weten hoe je beveiliging ervoor staat? Dankzij onze Cyber Security Assessment Tool (CSAT) ben je in no-time op de hoogte van alle digitale kwetsbaarheden en cyberrisico's voor jouw organisatie.

Neem contact op met QS solutions voor meer informatie of een afspraak:

T: +31 (0)33 – 71 22 111
E: marketing@qssolutions.nl

solutions