Veilig Zakelijk Internetten

Ben jij wel goed beveiligd?

De belangrijkste vragen voor mijn:

Netwerk- en systeembeheerder

Kun je mij de documentatie van mijn netwerk opleveren?

Welk antwoord mag u verwachten?

Doel van deze vraag is om inzicht te krijgen of de netwerkbeheerder en/of systeembeheerder een goed inzicht en overzicht heeft van wat er bij uw organisatie speelt op digitaal vlak. In de documentatie zou u in ieder geval de volgende gegevens moeten kunnen terugvinden:

- Lijst met de gebruikte apparatuur (server(s), werkplekken, switch(es), firewall(s), acces points, printers, internetverbindingen etc.).
- Lijst met de gebruikte applicaties.
- Inzicht in de plaatsen waar digitale koppelingen naar andere systemen liggen.
- Inzicht in de plaatsen waar (welke) data wordt bewaard.
- Autorisatiematrix (welke medewerkers zijn in welke gebruikers-groepen ingedeeld en welke gebruikersgroepen hebben rechten tot welke data).

Extra informatie

Deze vraag zal bij veel netwerk- en systeem beheerders de vraag oproepen of u hem wilt gaan verlaten (veelal wordt in dát specifieke geval de documentatie opgevraagd). Geef duidelijk aan dat dát niet het geval is, maar dat u het opvraagt in het kader van meer inzicht in de situatie van uw digitale omgeving te verkrijgen. Ú bent immers eindverantwoordelijk voor de (digitale) beveiliging!

Hoe wordt bij ons het onderhoud uitgevoerd (m.n. de installatie van patches en updates geïnstalleerd). Wie doet dit en wanneer gebeurt dit?

Welk antwoord mag u verwachten?

E.e.a. kan geautomatiseerd worden uitgevoerd óf er kan sprake zijn van handmatige patching / updating van systemen. Zorg er voor dat u te weten komt op welke wijze e.e.a. gecontroleerd wordt (is er een centraal systeem waarop wordt bijgehouden of alle werkplekken en servers wel up-to-date zijn en dat de patches/updates dus goed zijn uitgerold)? Is de beheerder ‘in-control’?

Extra informatie

Zorg er voor dat u duidelijkheid krijgt hoe dit plaatsvindt voor zowel besturingssystemen als voor de gebruikte applicaties.

Hebben wij een back-up procedure en kun je aangeven wanneer deze voor het laatste is getest, waarbij ook werkelijk is gekeken dat alle data van de back-up teruggezet kan worden?

Welk antwoord mag u verwachten?
Inzicht in de back-up procedure, d.w.z. wanneer worden er back-ups gemaakt en op welke momenten wordt gecontroleerd dat deze werken en ook teruggezet kunnen worden in het geval van een calamiteit. Zorg er voor dat u ook inzicht krijgt in de back-up van evt. databases (áls er wordt gecontroleerd op het kunnen terugzetten van een back-up, dan wordt er veelal alleen gecontroleerd of Office-data teruggezet kan worden. Veelal zijn juist in de databases zijn echter belangrijke gegevens opgeslagen).

Spreek verder door dat er een wachtwoord op de back-ups wordt gezet, dat de gegevens van de back-up alleen over beveiligde verbindingen wordt getransporteerd en dat de back-up versleuteld wordt opgeslagen.

Extra informatie
Bij een calamiteit zijn 2 dingen van belang, nl. de gegevens die verloren zijn gegaan op het moment van de calamiteit (in het geval van een dagelijkse back-up zal dit maximaal 24 uur zijn) en de tijd die het kost om weer up-and-running te zijn (hoe snel kan een back-up weer teruggezet worden). Uiteraard is dit laatste afhankelijk van het soort calamiteit (bij brand zal u meer tijd hebben om te herstellen dan bijvoorbeeld bij een crash van een server door bijvoorbeeld Ransomware). Spreek de verschillende scenario's dus met uw beheerder door.

Welke beveiligingsmaatregelen hebben wij getroffen voor mobiele werkplekken (laptops etc.)?

Welk antwoord mag u verwachten?
Er dient minimaal een (bij voorkeur gecentraliseerde) antivirus oplossing te zijn die periodiek wordt gecontroleerd op juiste werking. Daarnaast adviseren we om elke mobiele werkplek te voorzien van encryptie (versleuteling), VPN software (voor het geval er alleen openbare Wifi aanwezig is) en een moeilijk wachtwoord. Indien er met gevoelige/ bijzondere gegevens wordt gewerkt, is privacy-glas en eventueel slot (fysiek) aan te bevelen.

Extra informatie
Het kan zijn dat uw mobiele systemen nog niet allemaal zijn voorzien van de juiste beveiligingsmaatregelen. Overleg met uw beheerder welke (aanvullende) maatregelen genomen moeten gaan worden.

Wat is er binnen onze organisatie geregeld om er voor te zorgen dat we geen slachtoffer worden van ransomware?

Welk antwoord mag u verwachten?

Elke werkplek dient te zijn voorzien van antivirus. Uw bedrijfsnetwerk dient op het internet te zijn aangesloten via een goede firewall. Er dient een goed back-up- en recovery plan te zijn (als ransomware binnen uw organisatie actief is, dan is dat in feite de enige manier om uw bestanden weer terug te kunnen krijgen zonder het losgeld te hoeven betalen).

Zorg er daarnaast voor dat medewerkers goed geïnstrueerd worden rond het openen van E-mails, bijlagen, werken met USB sticks en het klikken op links op het internet (training). Denk hierbij bijvoorbeeld aan periodieke phishing simulaties.

Extra informatie

Ransomware is 1 van de meest voorkomende en schadelijke vormen van cybercriminaliteit. Ransomware zorgt er voor dat al uw bestanden versleuteld worden. Pas na betaling van losgeld (de ransom) ontvangt u – hopelijk – de sleutel om de data weer te ontsleutelen. Nadat u betaald heeft is het raadzaam om het hele netwerk opnieuw op te bouwen om te voorkomen dat de cybercriminelen achterdeurtjes hebben open gelaten om u opnieuw slachtoffer te laten worden (zeker als u betaald heeft, want ze weten dan dat u een ‘goede klant’ bent…).

Hoe weten we dat als een medewerker zijn laptop of een USB stick verliest we als organisatie geen datalek hebben?

Welk antwoord mag u verwachten?

Uit het antwoord moet blijken dat de beheerder ‘in-control’ is. Kunnen systemen vanaf afstand worden schoongemaakt? Kan de toegang vanaf systemen direct worden afgesloten? Wordt er gebruik gemaakt van encryptie (versleuteling) om er voor te zorgen dat áls een laptop of USB stick verloren raakt, er niet direct een datalek is? Zijn medewerkers getraind in wat ze moeten doen rond het werken met USB sticks of mobiele datadragers (bij voorkeur niet gebruiken) en laptops en het verlies daarvan?

Wat is het wachtwoordbeleid van ons op werkplekken, bij applicaties en bij belangrijke data?

Welk antwoord mag u verwachten?
Er dient een beleid te zijn waarin medewerkers op gezette tijden hun wachtwoorden moeten aanpassen. Daarnaast dient er een beleid te zijn voor het gebruik van een bepaalde lengte en/of moeilijkheidsgraad van wachtwoorden. M.n. de lengte van het wachtwoord is van belang (hoe langer, hoe lastiger te achterhalen voor een kwaadwillende). Overleg met uw beheerder hoe dit is ingeregeld.

Extra informatie
Voor systemen met gevoelige of bijzondere gegevens kunt u overwegen om te (gaan) werken met 2 factor authenticatie. Om bij uw systemen/ data/applicaties te kunnen komen moet een gebruiker iets weten (wachtwoord) en iets hebben (bijvoorbeeld een token). Pas als de gebruiker beide heeft kan hij/zij inloggen.

Kun je mij inzage geven in de logs van de afgelopen maand van de servers en netwerkcomponenten en kun je aangeven hoe we geregeld hebben dat vreemde situaties worden gemonitord en geëscaleerd?

Welk antwoord mag u verwachten?
Er moeten logbestanden van de meest kritische systemen (firewalls, switches, servers, applicaties) aangeleverd kunnen worden. Daarnaast moet er monitoring zijn ingeregeld, zodat er snel geëscaleerd kan worden indien zich vreemde situaties of calamiteiten voordoen.

De logs kunnen vertellen wat er exact is gebeurd en kan ook inzicht geven of er bij een cyber-inbraak data is buitgemaakt.

Maak duidelijke afspraken hoe lang de logbestanden worden bewaard en of alle logbestanden centraal verwerkt (gaan) worden. Zorg ook voor duidelijkheid rond het gebruik van systeemklokken (zodat de logs van alle systemen synchroon lopen).

Extra informatie
M.n. voor kleinere organisaties zal het kostbaar worden om 24x7 monitoring te laten uitvoeren. In plaats hiervan kunt u bijvoorbeeld ook afspreken dat de logs periodiek (bijvoorbeeld 1x per maand) worden doorgelopen om zo te kunnen achterhalen of zich vreemde situaties hebben voorgedaan.

De exacte inregeling zal per situatie anders zijn.

Zijn er afspraken gemaakt over het gebruik van BYOD (Bring Your Own Device) en cloud-gebasseerde oplossingen binnen ons bedrijf en houdt iedereen zich hieraan?

Welk antwoord mag u verwachten?
Er moet een duidelijk beleid zijn en hier moet naar gehandeld worden. Verder moet de netwerk-/systeembeheerder kunnen aantonen 'in-control' te zijn.

Extra informatie
Door een duidelijk beleid en afspraken te hebben rond BYOD en Cloud gebruik kunt u voorkomen dat gegevens/data 'zomaar' op straat komt te liggen, zonder dat u daar weet van heeft. Wat zijn de afspraken rond het gebruik van BYOD? Wordt er bedrijfsdata bewaard op systemen van medewerkers? Wat gebeurt er als zo'n systeem gestolen wordt of kwijt raakt? Is het missen van een persoonlijke telefoon direct een bedrijfsrisico? Is er specifieke beleid voor BYOD apparaten zodra ze verbinding maken met het netwerk van onze organisatie (moeten ze minimaal aan bepaalde eisen voldoen etc.)? Kunnen er 'zomaar' dropbox-achtige omgevingen in gebruik worden genomen, waardoor belangrijke data de organisatie kan verlaten? Welke afspraken zijn hierover gemaakt?

Wordt er binnen ons netwerk gebruik gemaakt van zonering / segmentering, bijvoorbeeld voor het gasten Wifi?

Welk antwoord mag u verwachten?
Indien u een gasten Wifi heeft dan zal dit ingeregeld moeten zijn/worden. Indien uw organisatie afdelingen heeft die absoluut niet bij elkaars gegevens mogen komen, dan kan het netwerk ook op andere punten gesegmenteerd zijn.

Extra informatie
Door gebruik te maken van segmentering in het netwerk kunt u bepaalde delen (segmenten) van het netwerk volledig afscheiden van andere delen. Dit is m.n. van belang indien u bijvoorbeeld Wifi ter beschikking stelt aan uw klanten/relaties. Stel dit Wifi in ieder geval ter beschikking via een apart gasten Wifi. Zorg er daarnaast voor dat dit volledig is afgescheiden van uw netwerk en eigen Wifi om te voorkomen dat een onbevoegde ook eenvoudig bij uw gegevens/data kan komen.

Wordt er periodiek een controle op kwetsbaarheden uitgevoerd om zeker te weten dat we geen online risico's lopen? Kun je mij rapportages van het afgelopen jaar opleveren?

Welk antwoord mag u verwachten?
Bij veel organisaties is een periodieke online controle op de kwetsbaarheid van het computernetwerk nog geen gemeengoed.

Schijf u in op www.veiliginternetten.nl/academy voor een gratis controle op uw website. Maak vervolgens een plan om een dergelijke scan periodiek uit te voeren en spreek dit door met uw beheerder.

We adviseren om minimaal jaarlijks een controle uit te voeren (voor kritische systemen vaker, bij voorkeur minimaal maandelijks).

Extra informatie
Per maand worden er wereldwijd zo'n 1.000 nieuwe kwetsbaarheden in hard- en software gevonden. Daarnaast kan het zijn dat een beheerder een foutje maakt, waardoor bijvoorbeeld een belangrijke poort op een firewall open komt te staan en gegevens eenvoudig vanaf het internet door een kwaadwillende kan worden benaderd.

Door de wetgever wordt geadviseerd om periodiek controles op kwetsbaarheden uit te voeren.

Op www.veiligzakelijkinternetten.nl/zakelijk kunt u een kosteloze test op uw website en bedrijfsnetwerk laten uitvoeren.

Laat de Cyber Risico Scan gratis uitvoeren!