WHITEPAPER

In 10 stappen naar ijzersterke digitale veiligheid

SCORE UTICA
THE CLOUD CONNECT COMPANY

SCORE UTICA
THE CLOUD CONNECT COMPANY

“Managers en bedrijfseigenaren willen een meer proactieve security aanpak, maar weten niet hoe”

Dat is de kop van een artikel dat onlangs verscheen.

Los van het feit dat we deze ‘**digitale pandemie**’ gezamenlijk moeten bestrijden en kennis moeten delen, ontkom je er als ondernemer niet aan om actief bezig te zijn met digitale veiligheid.

Om deze reden willen we je met deze whitepaper 10 concrete handvatten geven voor een flinke verbetering van de cybersecurity van jouw organisatie. Na het lezen van de 10 tips en stappen weet je waar de risico’s liggen en wat je concreet moet doen om risico’s te beperken. Zo zijn jij en jouw collega’s altijd up-and-running!

kpn partner network | strategisch partner

Microsoft Solutions Partner
Modern Work

Waarom kun jij met jouw bedrijf niet meer zonder een duidelijke cyber security aanpak?

- Microsoft geeft aan dat tussen juli 2020 en juni 2021 een toename is gemeten van **1070%(!) in ransomware** aanvallen.

- Gartner verwacht dat in 2024 driekwart van **alle CEO's persoonlijk verantwoordelijk** zal worden gehouden voor cyberbeveiligingsincidenten in bedrijven.

- **72% van de Nederlandse bedrijven** kreeg de laatste 12 maanden te maken met een cyberaanval.

- Met name **in het MKB is er een enorme toename in cyberaanvallen**. Dit komt doordat hackers er bij kleinere bedrijven vaak makkelijker mee weg komen. Dit gaat namelijk in mindere mate gepaard met media-aandacht en uitgebreide politie onderzoeken.

- Bedrijfsdata, persoonlijke informatie en documenten die op straat komen te liggen zorgen voor **reputatieschade** en hinderen jouw bedrijfsprocessen.

Als je om de genoemde redenen aan de slag gaat is het vanwege haalbaarheid en effectiviteit voor jouw organisatie van belang jouw security aanpak in lijn te brengen met de bedrijfsdoelstellingen. Het is de vraag hoeveel 'sloten' je op de fiets wil leggen. Een fiets met 10 sloten wordt minder snel gestolen, maar het duurt ook langer voor je zelf weer onderweg bent.

Wij adviseren om keuzes te maken op basis van risico inschattingen. Door goed met de onderwerpen in deze handleiding aan de slag te gaan ben je een stap voor ten opzichte van de meeste bedrijven en dat is al ontzettend veel waard. Hackers kiezen namelijk vaak de weg van de minste weerstand. Ze rammelen aan alle sloten en pakken de fiets die het makkelijkst open gaat. Daarna kijken ze pas wat er te halen valt.

Wij nemen je mee in 10 praktische tips en overwegingen, inclusief wat je daar **concreet nu** mee kan.

1. De kennis van jouw collega's

Je IT is zo sterk als de zwakste gebruiker, zeggen we bij Score Utica.

95% van alle hacks zijn mogelijk gemaakt door een menselijke fout. De methodes om inloggegevens of informatie te achterhalen worden steeds geraffineerder. Vroeger herkende je dochtertje van 3 waarschijnlijk al een 'nepmail' maar tegenwoordig zijn deze steeds moeilijker van echt te onderscheiden. Ze lijken steeds authentieker en ze worden persoonlijker. Om deze reden is het van belang dat medewerkers alert zijn en bij twijfel altijd verifiëren bij de betreffende persoon of instantie. Samen moeten ze er immers voor zorgen dat de continuïteit van je bedrijf gewaarborgd is. Dat betekent dat er geen geld wordt overgemaakt naar foute rekeningen en dat gevoelige informatie over je klanten, medewerkers en patenten/bedrijfsinformatie veilig is.

Hoe pak je dit concreet aan?
Vraag morgen aan 3 collega's of ze weleens een nepmail hebben gekregen of een verzoek tot het wijzigen van een wachtwoord en hoe ze daar mee om zijn gegaan. Aan de reactie kun je direct zien en vaststellen of ze weten hoe ze hiermee om moeten gaan. Neem contact met ons op om samen te bepalen hoe wij ervoor kunnen zorgen dat iedereen in de organisatie goed omgaat met digitale dreigingen.

2. Welke data heb je allemaal?

Data is het nieuwe goud! Grote tech spelers als Google en Meta (voorheen 'Facebook') maken er geen geheim van dat data de levensader is van hun businessmodel. Dit is direct de reden waarom inbraken in de 'normale wereld' afnemen en in de digitale wereld toenemen. Om deze reden is de basis dan ook het in kaart brengen van de data. Welke data heb je, welke is extra gevoelig en moeten wellicht aanvullend beschermd worden? Denk aan persoonlijke identificatiegegevens, financiële gegevens, assets, bedrijfsinformatie en productinformatie zodat je weet wat je moet beschermen.

Hoe pak je dit concreet aan?
Datalekken zijn helaas dagelijkse kost. Controleer dus ook eens of jouw emailadressen in eerdere lekken zijn voorgekomen en welke data is gelekt via deze tool. Zorg er daarnaast voor dat je precies weet welke data gevoelig is en beschermd moet worden.

3. Waar staat de data?

Vroeger lag het ‘goud’ in de kluis waar je alleen met een sleutel op locatie bij kon. In toenemende mate is hier de laatste jaren veel in veranderd. Tegenwoordig wil het grootste gedeelte van de medewerkers altijd en overal vanaf ieder device kunnen werken. Dan wordt het uitermate belangrijk om te weten waar je data staat en hoe het beveiligd is.

Hoe pak je dit concreet aan?
Beantwoord de volgende vragen:

- Welke applicaties heb je?
- Welke servers/diensten gebruik je om data op te slaan?
- Vanaf welke apparaten is bedrijfsdata beschikbaar?
- Stel de vraag: hoe zijn deze applicaties, data en apparaten beveiligd?

4. Hoe wordt de data gedeeld?

Een ander onderdeel van ‘het moderne werken’ is dat er steeds meer data gedeeld wordt, binnen én buiten de organisatie. ‘Insider threat’ is een term die je steeds meer hoort (bijvoorbeeld recent met een datalek bij de GGD). Het is van belang om te weten wie toegang heeft tot welke data en hoe deze data wordt gedeeld. Dit om datalekken te voorkomen en klanten en leveranciers zo veel mogelijk te kunnen garanderen dat jouw processen op een goede manier zijn ingericht.

Hoe pak je dit concreet aan?
Welke data deel je op welke manier met mensen van buiten de organisatie en zijn hier afspraken of restricties over? Beantwoord de onderstaande vragen:

- Mag alle data zomaar gedeeld worden, binnen of buiten de organisatie en zijn hier interne afspraken over?
- Mogen documenten met IBAN/creditcard/BSN-nummers überhaupt gedeeld worden?
- Gebruik je nog USB sticks en/of harde schijven of deel je alle documenten en bestanden via de cloud (Microsoft Teams en/of email)?
- Let op: de standaardinstellingen van SharePoint en Microsoft Teams zijn niet per definitie veilig. Breng dit in lijn met de standaard van jouw bedrijf en schakel experts in om met je mee te kijken waar dat nodig is!

5. Welke data is gevoelig en is de data versleuteld?

Encryptie is het versleutelen van informatie. Dit kan data zijn die opgeslagen staat op een laptop of harde schijf en/of data die verstuurd wordt. Door jouw data te versleutelen zul je de kans op menselijke fouten verkleinen. Afhankelijk van de situatie zijn hier uiteindelijk weer verschillende mogelijkheden voor waar wij je graag mee willen helpen. Zorg eerst dat je stap 2 t/m 4 in kaart hebt.

Hoe pak je dit concreet aan?

Beantwoord de vraag: welke data mag absoluut niet in verkeerde handen terechtkomen en is deze data al versleuteld? Hulp of advies nodig over hoe je jouw data kunt versleutelen of labelen? Neem contact op met een van onze experts!

6. Gebruik multifactorauthenticatie

Bij punt 3 hebben wij het gehad over data, applicaties en apparaten en hoe belangrijk de beveiliging hiervan is. Uit de Microsoft Secure Score, een tool waarin je kunt zien hoe veilig jouw organisatie op dit moment is en op welke plekken verbetering mogelijk is, blijkt dat multifactorauthenticatie (MFA) vaak de grootste winst oplevert. Met MFA combineer je iets wat je weet (code, wachtwoord), bent (vinger, gezicht, iris) en hebt (telefoon, email, hardware token). Daarmee is veel te voorkomen. Omdat het wachtwoord de zwakste schakel is sturen wij met Microsoft zelfs op passwordless MFA, dus alleen iets wat je bent en iets wat je hebt. Bij sommige applicaties ontkom je er nog niet aan om met een wachtwoord te werken. Bij veel bedrijven is er nog weerstand voor MFA omdat je extra handelingen moet uitvoeren voor je aan de slag kunt. Door slimme technieken kunnen wij ervoor zorgen dat je op veilige momenten niet altijd al die handelingen hoeft te doen zodat je snel kunt inloggen.

Hoe pak je dit concreet aan?

- Het allerbelangrijkste is: stel direct multifactorauthenticatie in voor Microsoft 365 en al jouw belangrijke applicaties.
- Moet je toch een wachtwoord gebruiken? Gebruik dan lange wachtwoorden (wachtzinnen het liefst) die niet eerder gelekt zijn.
- En is er een duidelijk beleid over waar een wachtwoord aan moet voldoen?
- Neem contact met ons op als wij je kunnen helpen met veilig inloggen en de verschillende manieren die daarvoor zijn.

7. Voer updates direct uit en houd het bij

Hoe vaak zie je een melding dat er een update klaar staat, voor Windows bijvoorbeeld? En hoe vaak stel je deze uit? Het uitstellen van updates is gevaarlijk! Updates dichten namelijk veel lekken in software waarmee hackers in kunnen breken. Het is belangrijk om hier afspraken over te maken om te voorkomen dat medewerkers achterhaalde, onveilige systemen of software gebruiken. Denk hierbij niet alleen aan je computer maar ook aan computerprogramma's, browser, apps op je telefoon en slimme apparaten. De ransomware aanval 'WannaCry' wordt omschreven als de 'ergste ooit' (bron: AVG) en saillant detail? Deze kon tot stand komen door een lek in Windows en had voorkomen kunnen worden door tijdig updaten door de gebruikers.

Hoe pak je dit concreet aan?

Beantwoord de volgende vragen:

- Is er een beleid over updates?
- Kunnen gebruikers updates uitstellen?
- Zo ja, zorg er dan voor dat hier een duidelijk beleid over komt, want: een dag updates uitstellen is een dag langer gevaar lopen.

8. Het belang van het bedrijfsnetwerk

Vertrouw je alles binnen je bedrijfsnetwerk of wil je hier ook zaken verifiëren? Wie heeft allemaal toegang tot dit netwerk en zijn er goede scheidingen aangemaakt tussen bijvoorbeeld het gastennet en het bedrijfsnetwerk? En gebruik je goede beveiliging zoals een moderne firewall om aanvallen in je hele netwerk zowel te kunnen detecteren als bestrijden?

Hoe pak je dit concreet aan?

- Is er een gastennetwerk aanwezig?
- Zo ja, is deze volledig fysiek afgescheiden van het hoofdnetwerk?
- Zijn de wifi access points, routers en switches goed beveiligd en up-to-date?
- Weet je dit niet zeker of is het antwoord 'nee'? Neem contact op voor een vrijblijvende netwerkscan op locatie voor 100% inzicht!

9. Bescherm jouw apparaten

Met name door het hybride werken wat inmiddels volledig is omarmd, is het niet alleen belangrijk je bedrijfsnetwerk te beveiligen maar ook te kijken naar alle apparaten binnen de organisatie (bijvoorbeeld pc's, laptops, tablets, scanners, wifi-punten etc.). Kortom: welke apparaten gebruik je (privé en zakelijk) en hoe zijn deze beveiligd?

Gebruik je nog een traditionele antivirus of een 'next generation' tool? Een traditionele antivirusscanner checkt of het een bekend virus tegenkomt, maar een next gen antivirus analyseert afwijkingen in gedrag op basis van big data en kunstmatige intelligentie en zal je daardoor eerder helpen hackers voor te blijven. Next gen is tegenwoordig onmisbaar, gezien het toenemende aantal nieuwe virussen en manieren om bij bedrijven binnen te komen.

Hoe pak je dit concreet aan?
Ga na hoe jouw apparaten zijn beveiligd en hoe virussen worden behandeld. Bepaal of het tijd wordt voor een nieuwe tool om nieuwe dreigingen écht voor te zijn.

Extra tip: veel bedrijven gebruiken maar een klein deel van security toepassingen die beschikbaar zijn in een Microsoft 365 licentie. Wij gaan graag met je in gesprek om te bepalen of je optimaal gebruikmaakt van de diensten die je nu al afneemt.

10. Wat als het mis gaat?

Als het dan toch mis gaat en er is brand, je bent gehackt of je hebt te maken met ransomware is het belangrijk dat je weet wat je moet doen. Zorg voor de juiste procedures om bij security incidenten weer zo snel mogelijk up-and-running te zijn.

Hoe pak je dit concreet aan?
Stel aan 3 collega's de vraag: wat moet je doen als je wordt gehackt en je ziet op jouw scherm dat je de controle kwijt bent? Aan de hand van de antwoorden kun je inschatten wat de afspraken moeten worden. Maak bijvoorbeeld afspraken over wat je moet doen wanneer er brand uitbreekt, wanneer je hebt gereageerd op een nepmail of wanneer je vertrouwelijke informatie bent kwijtgeraakt.

Het is belangrijk dat je iemand verantwoordelijk stelt om mee te schakelen bij incidenten. Dit kan iemand van binnen de organisatie zijn of iemand van Score Utica.

Zorg er verder voor dat de back-up van jouw data 'off-site' staat, dus op een andere plek dan de kantoorlocatie. Test het terugzetten van de data periodiek. Hoe lang duurt het om vanuit de back-up weer up-and-running te zijn?

De volgende stap?

Uiteindelijk geloven we er bij Score Utica in dat je moet starten met een solide basis van de IT infrastructuur. Onder andere daarom standaardiseren wij tegenwoordig grotendeels op Microsoft. Microsoft investeert namelijk 3.500 security medewerkers en 4 miljard dollar per jaar in security wat je kansen aanzienlijk vergroot om altijd één stap voor te blijven op hackers en andere digitale dreigingen.

Misschien heb je na het lezen van de 10 bovenstaande punten nog vragen of twijfels. Wij gaan graag de dialoog met je aan om jou te helpen met jouw digitale veiligheid. Wij kijken graag samen met jou naar hoe wij security kunnen automatiseren zodat jij minimaal omkijken hebt naar security. Op die manier kan jouw bedrijf zich blijven focussen op de business en kerntaken en hoef je 's nachts niet wakker te liggen vanwege zorgen over digitale veiligheid!

Vertel mij meer

SCORE UTICA
THE CLOUD CONNECT COMPANY

Wij denken graag met je mee

Plan een afspraak of een call met ons in als we jou verder kunnen helpen met security of kunnen helpen om te zorgen dat jouw organisatie altijd, en overal, vanaf ieder device op een veilige manier kan werken.

Bekijk ook onze Modern Workplace, de veiligste werkplek waar je blij van wordt met alle tools die je nodig hebt om veilig te kunnen werken!

Kennismaken **Naar Modern Workplace**

kpn partner network | strategisch partner

Microsoft Solutions Partner
Modern Work