Security-instructies

Wat je kunt doen als organisatie

Cybersecurity: de basis op orde

Cybersecurity was altijd al belangrijk, maar vandaag de dag moet het topprioriteit zijn binnen je organisatie. We zien dit aan onze business-cijfers en de onderzoeken bevestigen dit beeld. Het aantal 'ongeoorloofde aanmeldverzoeken', hacks, phishingmails, datalekken en andere security-risico's neemt namelijk toe.

Maar waar start je? Maak de basis in orde. Dan is de kans een stuk kleiner dat je slachtoffer wordt van cybercrime. Maar wat is die basisbescherming? Hier vind je de eisen die wij minimaal stellen om een organisatie de stempel 'goed beveiligd' mee te geven. Als organisatie moet je onderstaande punten op z'n minst geregeld hebben. Alvast excuses voor de dure woorden, maar soms komen we er niet onderuit.

Wachtwoordbeleid

Sterke wachtwoorden zijn absoluut noodzakelijk binnen je cybersecurity. Makkelijke wachtwoorden zijn voor hackers vaak binnen enkele seconden te kraken. Maak daarom een beleid hoe met wachtwoorden om te gaan. Zorg bijvoorbeeld dat je een wachtwoord nooit meerdere keren gebruikt op verschillende apps/websites. En zeker niet het wachtwoord welke je gebruikt om in te loggen op je werk. Een complex wachtwoord (letters/leestekens en cijfers) is een must en deze dient regelmatig gewijzigd te worden.

Multifactor authenticatie (MFA)

Het is een van de meest effectieve cybersecuritymaatregelen die je als bedrijf kunt treffen: tweefactor authenticatie. Bij deze inlogmethode combineer je twee verschillende factoren, bijvoorbeeld iets dat de gebruiker weet (een wachtwoord of pincode) en heeft (zoals een telefoon of token). Wil je het echt solide aanpakken? Dan kies je voor multi-factor authenticatie. Denk bijv. aan Face-ID in combinatie met telefoon en pincode. Pas dit toe op alle verbindingen die je maakt naar lokale of cloud netwerken. Zo weet je dat degene die inlogt, ook echt daadwerkelijk degene is die mag inloggen.

Enterprise Mobility Management

Door het thuiswerken is het gevaar rondom mobiele apparaten toegenomen (de zogenoemde endpoints). Met Enterprise Mobility Management kan je deze centraal beheren en daardoor op afstand configureren en beveiligen. Denk hierbij aan zaken als op afstand wissen of vergrendelen bij diefstal, verplichte versleuteling toepassen, toestaan/weigeren van applicaties etc. Meer weten over het beheren van devices? Lees hier meer.

Gebruik-beleid

Maak afspraken omtrent het werken op kantoor, thuis en op afstand. Bepaal bijvoorbeeld vanaf welk device er gewerkt mag worden? Privé laptop? Zakelijke laptop? Mag er data gekopieerd worden? Lock je scherm als je even van je plek wegloopt. USB-sticks moeten die wel of niet geblokkeerd worden etc. Kortom, definieer spelregels waar een gebruiker zich aan moet houden en richt de omgeving ook zo in. Met de eerdergenoemde Enterprise Mobility Management kunnen dit soort spelregels ook afgedwongen worden. Resultaat: grip op de data van de organisatie.

Cybersecurity-verzekering

Een hack kan veel schade aanrichten voor een organisatie. Denk aan de kosten van het 'dichten' van het lek. Het bedrijf staat letterlijk stil. Er raakt essentiële data verloren. Maar vooral de kosten die ontstaan door omzetverlies en/of reputatieschade. Alles bij elkaar kan het veel geld kosten. Soms zoveel dat het organisaties de kop kost. Gelukkig zijn er tegenwoordig verzekeringen die hier onderdelen in dekken. Zorg dus voor een goede cybersecurity-verzekering.

Opleiden van medewerkers en organisatie breed beleid

Al grappend wordt in ICT-land vaak gezegd: de kwetsbaarheid zit tussen het scherm en de bureaustoel. Helaas is dit wel waar. Mensen worden gezien als de zwakste schakel in cybersecurity. Gezien de

aanvallen steeds geavanceerder worden, is het belangrijk om medewerkers basiskennis over cybersecurity bij te brengen en up to date te houden. Denk aan tips als: open geen onbekende uitvoerbare programma's en wees alert voor phishing. Ook is het goed om organisatie breed een beleid op te stellen, met bijvoorbeeld regels als: log niet in op openbare wifinetwerken en sla geen bedrijfsdocumenten op in de publieke cloud. Kortom, je moet hier structureel aandacht aangeven intern. Wij doen dit door middel van een adoptie en security awareness programma voor het team.

Software-updates

Kwetsbaarheden in software zijn als open deuren binnen je bedrijf. Dit is een van de grootste oorzaken tot succesvolle hacks. Zorg dus dat je altijd de laatste updates (en upgrades) van besturingssystemen en (mobiele) applicaties hebt geïnstalleerd. Denk bijvoorbeeld aan verouderde besturingssystemen zoals Windows XP, 7 en 8, Windows Server 2003, 2008 etc. Zorg ervoor dat je dit proces van updates borgt door periodieke checks en automatische alerts.

Supported hardware

Zorg ervoor dat alle hardware binnen officiële ondersteuning van de leveranciers valt. Hiermee staat de leverancier garant voor doorontwikkeling van het product en de support hierop. Hierdoor ben je verzekerd van o.a. firmware updates.

Back-uppen

Voorkomen is altijd (veel) beter dan genezen, maar het is wel fijn dat je eventueel kúnt genezen als je slachtoffer wordt van cybercrime. Back-ups zorgen ervoor dat je na een cyberaanval of crash snel weer aan de slag kunt. Wist je bijvoorbeeld dat de Microsoft 365 omgeving standaard niet geback-upt wordt door Microsoft? De back-up van deze data moet je geregeld hebben.

Voorkom shadow-IT

Het gebruik van cloud-oplossingen is wijdverspreid. Werken in de cloud is onmisbaar bij het werken op afstand, om data te delen en online samen te werken. Het zorgt voor een boost in de productiviteit en betere communicatie. Goed nieuws, zolang je organisatie maar goed in beeld heeft welke cloud-applicaties precies gebruikt worden. Vaak maken medewerkers ongemerkt gebruik van ongeautoriseerde applicaties. Dit kunnen apps zoals Dropbox, WeTransfer, iCloud etc zijn. Hier ligt het gevaar van zogenoemde 'Shadow IT' op de loer. Door gebruik van de apps weet je niet meer waar de data van de organisatie zich bevindt. Met de inzet van Enterprise Mobility Management kan je centraal managen wat een device wel en niet kan.

Managed firewall

Een firewall is essentieel om te zorgen dat jouw bedrijfsnetwerk veilig is. Deze zorgt ervoor dat al het verkeer van buiten naar binnen en vice versa wordt gecontroleerd op dat dit mag en veilig is. Het juist instellen en onderhouden vraagt veel expertise en is een continu proces. Steeds meer bedrijven kiezen daarom voor een managed firewall. Het voordeel? Wij zorgen dat de firewall altijd up to date is en wordt gemonitord voor een vast bedrag per maand.

WiFi netwerk

WiFi is niet meer weg te denken en wordt veel gebruikt. Belangrijk om ervoor te zorgen dat je dit op een veilige manier beheert. Waar moet je dan aan denken? Een gastennetwerk op kantoor is bijvoorbeeld een must. Zorg hierbij dat het verkeer via de firewall gescheiden wordt van het kantoornetwerk. Maar kijk ook naar wie op het netwerk mag. Zo kun je bijvoorbeeld instellen dat alleen geregistreerde zakelijke devices op het netwerk mogen. Verder iets heel simpels als het regelmatig wijzigen van het wachtwoord van het WiFi netwerk. Met de juiste maatregelen houd je controle en hackers buiten.

Branchespecifieke maatregelen

Cyber security is in sommige branches zelfs topprioriteit. Denk aan de informatiebeveiliging in de zorg. Als de gegevens uit zorgsystemen op straat belanden, is de privacy van de betrokkenen ernstig beschadigd. Daarom is er een norm ontwikkeld: NEN 7510. Als je deze richtlijn volgt, is het voor iedereen duidelijk dat je professioneel omgaat met informatiebeveiliging in de zorg. Weten of er specifieke wet- en regelgeving voor informatiebeveiliging in jouw branche bestaat? Je kunt het vinden op nen.nl.

Algemene Verordening Gegevensbescherming (AVG)

Onder de basisbescherming van je data valt ook de manier waarop je persoonsgegevens verwerkt. Heb je een klantenbestand of een personeelsadministratie? Dan verwerk je al persoonsgegevens. En moet je je sinds 2018 houden aan de Algemene Verordening Gegevensbescherming (AVG). In deze Europese wet staat wat je allemaal mag doen met persoonsgegevens en hoe je deze gegevens moet beschermen. De AVG geldt voor verwerkingen die (deels) automatisch gaan. Bijvoorbeeld verwerkingen in een computer of database. Meer informatie over de AVG vind je hier.

Meer over DB+

DB+ zit vol op service. En dat doen we vanuit een sterk samenhorigheidsgevoel: een klant is niet zomaar een klant. Net zomin als dat DB+ zomaar een bedrijf is. Natuurlijk, we bieden geïntegreerde telecom en IT-oplossingen op maat. En we nemen je net zo makkelijk alles uit handen als dat we enkel een basisoplossing leveren.

Maar waar we echt in uitblinken is onze werkwijze. Hierop lopen we namelijk echt op de troepen vooruit. Aandacht is hier het toverwoord. Aandacht is mooi, aandacht is schaars. Vandaar dat we onze volle aandacht schenken aan bedrijven en mensen met wie we een klik hebben.

Ook al leven we in een digitale wereld, goed persoonlijk contact is nog steeds superbelangrijk. Want hoe goed je bedrijfsplan ook is, het zijn de mensen die de organisatie succesvol maken.

Samenwerking met Veneco

Wij voorop, jij voorop

De vraag uit de markt is duidelijk: bedrijven willen één leverancier voor hun telecom en IT. Niet zo gek, want met hoe meer partijen je werkt, hoe groter de kans op ruis in techniek en communicatie. Door onze fusie met Veneco kunnen we je straks alles aanbieden. Al je telecom- en IT-oplossingen in één slim ecosysteem. Snel, gebruiksvriendelijk en klaar voor de dag van morgen. Zo loop jij voorop in je markt. En ja, wij ook in de onze.

Meer weten over de samenwerking

Contact

DB+
Naaldwijkseweg 100
2291 PA Wateringen

Telefoon: 0174 – 316060
E-mail: info@dbplus.nl