datect

Hoe het MKB zich kan beschermen tegen cyberaanvallen!

Het is lastig om in te schatten hoe kwetsbaar jouw bedrijf is voor cyber-criminelen. Wij leggen je uit waarom jouw bedrijf kwetsbaar is, en hoe jij jezelf kan beschermen.

Zo gaan cybercriminelen te werk

Cyberaanvallen, bijvoorbeeld door middel van Ransomware, zijn bezig aan een sterke opmars. Bedrijven worden steeds vaker geconfronteerd met versleutelde netwerkapparatuur, harde schijven en data. Daarnaast blijken back-ups ook geïnfecteerd te zijn. Dat komt bijvoorbeeld doordat de netwerken van veel organisaties aan elkaar gekoppeld zijn, bijvoorbeeld omdat zij werken in een supply chain, en er onvoldoende maatregelen geïmplementeerd zijn.

Een aanval op het ene bedrijf betekent dan vaak ook een aanval op bedrijven in de verdere waardeketen. Veel aanvallen beginnen met een phishingmail waarbij gebruikers nieuwsgierig gemaakt worden om bijvoorbeeld een bestand te downloaden of op een bepaalde link te klikken. Eenmaal geklikt is dit het begin van bijvoorbeeld een ransomware aanval.

Daarnaast wordt het cybercriminelen ook steeds gemakkelijker gemaakt. Enerzijds omdat de opsporing een moeizaam proces is, maar ook omdat er op het "dark web" kant-en-klare modules te koop zijn die cyber criminelen kunnen kopen om hun aanvallen uit te voeren. Hier gaan grote bedragen in om. Dat verklaart voor een groot deel de toename van aanvallen.

Het *3 lines of defence* model van Datect

Ons 3 lines of defense model helpt ondernemers met het opbouwen van een basisstructuur voor informatiebeveiliging.

Het model legt de basis voor een effectieve bescherming.

Basis op orde

Voor ieder type bedrijf, ongeacht omvang of sector, is het belangrijk 9 basismaatregelen op het gebied van informatiebeveiliging toe te passen. We lichten ze stap voor stap toe.

1.AUTORISATIE MODEL

Door gericht autorisaties op te zetten voorkom je bijvoorbeeld dat alle gebruikers beheerder zijn binnen een systeem. Denk goed na over wie welke rechten nodig heeft en minimaliseer de uitgifte van beheerdersrechten. Belangrijk is om ervoor te zorgen dat je het model afstemt op de structuur van je organisatie. Misschien nog wel belangrijker: zorg ervoor dat je het model onderhoudt.

Door tweestapsverificatie of Multi-Factor Authenticatie (MFA) in te schakelen creëer je een extra authenticatiestap boven op je gebruikersnaam en wachtwoord. Dit maakt de toegang tot je systemen veel veiliger en minder gevoelig voor cyberaanvallen. Ons advies: activeer dit altijd waar het kan, maar zeker voor je beheerdersaccounts of andere accounts met hoge systeemrechten.

2.BEHEERDERSRECHTEN

Ook administratieve rechten voor een netwerkdomein zijn vaak een heikel punt. Neemt een cybercrimineel de werkplek over van een gebruiker die beheerrechten binnen het netwerk heeft? Dan kan hij eenvoudig overal bij en zonder moeite alle systemen versleutelen. Zorg er dus voor dat beheerdersrechten altijd goed afgeschermd zijn en gebruik deze alleen als het echt nodig is.

3.VERSLEUTELEN VAN GEVOELIGE INFORMATIE

Informatie is voor veel bedrijven erg belangrijk. Natuurlijk wil je dit zo goed mogelijk beschermen door middel van bijvoorbeeld toegangscontrole en een autorisatieconcept. Daar bovenop is het aan te raden cruciale informatie te voorzien van versleuteling (encryptie). Mocht er dan toch ongeautoriseerde toegang plaats vinden en de versleutelde informatie of data wordt gestolen, dan kunnen de criminelen de informatie niet lezen zonder dat zij de juiste sleutel hebben. Zorg er dus voor dat je de sleutel niet opslaat bij je data op het netwerk.

4.ANTI-VIRUS EN ANTI-MALWARE IMPLEMENTATIE

Dagelijks komen er nieuwe virussen en malware bij. Het is enorm belangrijk om een goede antivirus en malware detection engine op al je systemen te hebben installeren en op een juiste manier te configureren. Daarnaast moeten er dagelijks nieuwe antivirus definities worden geïnstalleerd. Dit is in veel gevallen een geautomatiseerd proces waardoor het risico op een virus of malware aanval verkleind wordt.

5.SYSTEMATISCH BACK-UPS MAKEN EN REGELMATIG TESTEN

Het spreekt misschien voor zich, maar in de praktijk worden er vaak geen back-ups gemaakt, en worden gemaakte back-ups niet gecontroleerd op volledigheid en functionaliteit. In beide scenario's ben je erg kwetsbaar voor ransomware aanvallen. Als je goedwerkende back-ups hebt, ben je weerbaarder wanneer je bijvoorbeeld slachtoffer wordt van een ransomware aanval. Als dan ook je data nog versleuteld is, sta je een stuk sterker.

6.HET PROCESMATIG INSTALLEREN VAN SOFTWARE UPDATES EN PATCHES

Patchen, patchen en nog eens patchen. Dagelijks komen er, net zoals virussen, nieuwe kwetsbaarheden in software uit. Deze moeten zo snel mogelijk gepatched of geüpdatet worden. Richt een proces in waarbij dit regelmatig gecontroleerd uitgevoerd wordt en waarbij je ook de mogelijkheid en flexibiliteit hebt om "nood" patches te installeren. Die eigenlijk niet kunnen wachten. Door dit proces goed ingericht te hebben, versterk je je defensiemodel.

7. REDUCEER HET AANVALS-OPPERVLAK VANAF HET INTERNET

Er was een tendens dat we zo'n beetje de gehele interne infrastructuur wilden koppelen aan het internet. Gelukkig zijn we grotendeels van dat concept afgestapt: veel aan het internet gekoppelde systemen zijn slecht of onvoldoende beveiligd en geconfigureerd, waardoor ongeautoriseerde toegang vanaf het internet nog steeds mogelijk is. Zorg ervoor dat je interne ICT-omgeving zo minimaal mogelijk gekoppeld is aan het internet. Hiermee verklein je het aanvalsoppervlak vanaf het internet, en daarmee het risico op ongeautoriseerde toegang. Daarnaast is het verstandig om gebruik te maken van technieken en oplossingen als DMZ (Demilitarized Zones), firewalls, proxyservers en reverse proxyservers. Maak dus een veilig ICT ontwerp.

8.SEGMENTEER HET NETWERK ZOVEEL MOGELIJK

Natuurlijk ben je als ondernemer altijd op zoek naar de meest optimale inrichting van je ICT-netwerken. Je wilt dat je medewerkers overal snel bij kunnen, zonder lastige extra stappen. Toch loont het om je netwerk te segmenteren. Zonder het opdelen van je netwerk is het voor hackers eenvoudiger om je complete netwerk over te nemen en bestanden te gijzelen of te versleutelen.

Het opdelen van je netwerk kun je vergelijken met het plaatsen van branddeuren om te voorkomen dat een brand letterlijk als een lopend vuurtje door je het bedrijfspand gaat. Medewerkers toegang geven tot netwerken en bestanden op een 'need to know' basis helpt al om een effectieve netwerksegmentatie te ontwerpen.

9.SECURITY AWARENESS

Zorg dat medewerkers aanvallen herkennen en weten hoe ze ermee moeten omgaan. Dat noemen we security awareness. Het is van cruciaal belang dat medewerkers instructie en training krijgen op het gebied van security awareness en hoe ze moeten handelen in diverse aanvalsscenario's. De kracht van herhaling is hierbij het sleutelwoord. Security awareness train je op verschillende manieren zoals phishing campagnes, instructies en/of sessies, online trainingen, etc. Een maandelijkse nieuwsbrief waarbij aandacht gegeven wordt aan het onderwerp is een goed begin. Bedenk wel dat er actieve aandacht en met een herhalend karakter nodig is om het onderwerp levend te houden en de risico's te verlagen.

Netwerkmonitoring

Nu je in de basis de minimale maatregelen hebt getroffen, is het belangrijk om in de gaten te houden wat er nu precies op je netwerk gebeurt. Vaak zijn cybercriminelen langere tijd bezig om uit te vinden of er toch niet ergens een zwak punt van de beveiliging te vinden is.

Opvallend gedrag wordt door goede netwerkdetectie ontdekt. Het is belangrijk dat je serieuze bedreigingen herkent. Weet dat er waarschijnlijk dagelijks wel een poging wordt gewaagd door cybercriminelen, maar gelukkig is het niet altijd serieus of zorgelijk. Het probleem bij veel bedrijven is dat ze het vermogen (kennis en/of capaciteit) missen om criminelen en ransomware in een vroegtijdig stadium te ontdekken.

Zorg in ieder geval voor goede logging tools en detectiesoftware. Ook hier geldt: hoe eerder je verdachte activiteiten binnen je netwerk signaleert, des te eerder kun je ingrijpen.

Disaster Recovery Plan

Je hebt nu de basis op orde, je houdt in de gaten wat er gebeurt op het netwerk en je reageert natuurlijk adequaat op gevaar. Hiermee heb je het risico van een succesvolle aanval al aanmerkelijk gereduceerd. Toch lukt het criminelen soms om binnen te komen.

Zonder een goed noodplan verlies je kostbare tijd. En juist de eerste uren nadat het incident ontdekt is, zijn cruciaal. Het is zonde als je eerst tijd moet steken in de organisatie van een crisisteam. Met een goed noodplan, dat minimaal 1 keer per jaar is geoefend, beperk je de schade van een incident aanzienlijk. Neem in het noodplan ook je ketenpartners mee. De kans is namelijk aanwezig dat je via hen geïnfecteerd wordt of juist andersom.

datect

En wat nog meer?

Met de inrichting van het 3 lines of defense model ben je al een heel eind op weg. In de basis heb je het nu goed georganiseerd. Maar, **“the proof is in the pudding”.** Maak er geen project van, maar zorg dat de management-cyclus met betrekking tot jouw informatiebeveiliging goed is ingericht.

Voer minimaal jaarlijks een risico-analyse uit, test de techniek via een security- of penetratietest en zorg dat je medewerkers de risico’s kennen en herkennen. In onze volgende whitepaper gaan we dieper in op de managementcyclus met betrekking informatiebeveiliging.