Perfect Day

Niet in cyber security investeren?

Zo tackle je de meest gehoorde excuses.

www.perfectday.nl

“Mijn bedrijf is heus niet interessant voor cybercriminelen”. Het is een veelgehoord argument van ondernemers om niet aan de slag te gaan met cybercriminaliteit. Of: “Bij ons valt er toch niets te halen”.

Helaas voor hen hebben zij slechts gedeeltelijk gelijk. Het klopt, een cybercrimineel is meestal niet geïnteresseerd in bestanden van de ondernemer. Maar zij weten één ding heel goed: die bestanden zijn voor de ondernemer van vitaal belang. En dat buiten cybercriminelen uit. Door losgeld te vragen voor het decrypten van de systemen en het vrijgeven van belangrijke bestanden. Veel ondernemers onderschatten de impact van een hack. Wij horen van de vele verzekeringsadviseurs waarmee wij werken dat zij dit dagelijks ondervinden in hun werk. Wij hebben dit document opgesteld om je te helpen de meest gehoorde excuses te tackelen die ondernemers gebruiken om niet in cybersecurity te investeren.

1. “Mijn IT-leverancier regelt de cyber security”

Mkb-bedrijven besteden hun IT & OT vaak uit. Over het algemeen wordt de IT-leverancier verantwoordelijk gemaakt voor:

- Hardware (computers, printers etc.)
- Software
- SaaS-providers (vormgeving software, CRM, CMS etc.)
- Cloud-providers (Google Cloud, Microsoft Azure etc.)
- Netwerkbeheer
- Website en hosting

Meestal is het niet reëel om van de IT-leverancier te verwachten dat hij zonder nadere afspraken ook verantwoordelijk is voor de cybersecurity van de services. Doorgaans leveren IT-leveranciers de digitale infrastructuur en technische basismaatregelen. Denk hierbij aan firewalls, antivirus scanners, endpoint security, backup faciliteit en patching (updaten geleverde software).

De IT-leverancier is over het algemeen niet verantwoordelijk voor de security van de website, overige Cloud storage van Saas platformen en IoT (Internet of Things, slimme apparaten). Terwijl de diensten wel direct in verbinding staan met het netwerk.

De vraag is dus: wat is afgesproken met de IT-leveranciers over security en welke partij is waarvoor verantwoordelijk? De IT-leverancier is een belangrijke schakel, maar ook hij is geen tovenaar! Het is daarom ook belangrijk dat in de scope van de overeenkomst, duidelijk omschreven is, of en in hoeverre de IT-leverancier verantwoordelijk is voor cyber security. En voor welk deel hiervan.

Laat de ondernemer dit aan zijn/haar IT-leverancier vragen:

- Op welke wijze is mijn bedrijf goed beveiligd?
- Wat is ons meest kwetsbare punt in de cyberbeveiliging?
- Welke data is het meest interessant voor criminelen en/of concurrenten?
- En hoe goed is de data uit het punt hierboven beveiligd?
- Hebben wij een noodplan in geval van hack of datalek?
- Hoe bewijst de IT-leverancier of zij hun cyber security op orde hebben?
- Heeft de IT-leverancier weleens een onafhankelijke audit laten doen?
- Is de IT-leverancier gecertificeerd?
- Hoe zit het met de andere onderdelen zoals AVG, Medewerkers, Noodprocedure, Ketenveiligheid en de website?
- Doet de IT-leverancier restore tests van de backups? Is er een updatebeleid? Doen zij monitoring, Mobile Device Management? Zorgen zij voor veilige werkplekken ook thuis?

Dit zien wij in de praktijk...

- Een onderneming heeft al zijn hardware en systeemsoftware door ICT-leverancier X laten installeren. In het servicecontract is opgenomen dat de patches (updates) 1 keer per zes maanden worden gedaan. Op 30 mei heeft een update plaatsgevonden en op 30 juni wordt een nieuwe versie van de software met security-updates uitgegeven. De komende 5 maanden is het bedrijf extra kwetsbaar voor een inbraak op de systemen. Veiligheidslekken in systeemsoftware zijn immers wereldwijd bekend.
- De klant besluit uit kostenoverwegingen geen beheer op te nemen in het pakket. Dit betekent dat hij zelf verantwoordelijk is voor (beveiligings-) updates. Door de waan van de dag in het bedrijf komt hij er niet aan toe, laten updates maanden op zich wachten en wordt hij gehackt.
- We zien maar al te vaak dat de IT-beheerder wel zorgt dat er back-ups worden gemaakt, maar dat er geen restore tests worden uitgevoerd. Hij komt er pas achter dat de procedure niet goed is ingericht op het moment dat een back-up tijdens een noodsituatie teruggezet wordt. Helaas is het dan te laat. Test daarom altijd met back-uppen én het terugzetten ervan.
- De IT-leverancier zorgt er niet voor dat de onderneming voldoet aan de AVG. In bepaalde vormen van dienstverlening zullen aspecten van de AVG mee zijn genomen. De ondernemer is zelf verantwoordelijk voor het totaalbeeld.
- De IT-leverancier zorgt ook niet voor awareness bij medewerkers. Bijvoorbeeld dat ze weten welke gegevens ze wel en niet mogen delen, slim wachtwoordgebruik en herkennen van phishing mails.
- Veel ondernemers vertrouwen erop dat hun IT-leverancier zich ook bekommert om cyber security. Dit is echter niet vanzelfsprekend.

2. “Al mijn data staat in de Cloud”

Oke, hier kunnen we kort over zijn: de cloud is niet zonder meer veiliger dan lokale opslag. Cloud-providers als MS Office, Google en Icloud, maar ook SaaS oplossingen als Exact en Salesforce etc. zullen er alles aan doen jouw data te beschermen. Maar je maakt nog steeds contact via je eigen, lokale apparaten waardoor malware in de cloud omgeving terecht kan komen en schade kan aanrichten. Let vooral op met kleinere onbekende cloud-providers en de locatie daarvan. De beveiliging is niet zelden beneden de maat en daarmee een aantrekkelijk doelwit voor criminelen. Omdat ze met relatief weinig inspanning de gegevens van meerdere bedrijven tegelijk te pakken kunnen krijgen.

Het is dus geen vaststaand feit dat de cloud veiliger is. De cloud brengt andere beveiligingstechnieken met zich mee. Bij cloudaanbieders zelf gaat het ook regelmatig mis (MS, Google, Amazon) en lekt data of gaat data verloren. Dus help de ondernemer om risico’s in kaart te krijgen met de volgende vragen:

Heeft de ondernemer ook hieraan gedacht?

- → Heeft de ondernemer een verwerkersovereenkomst met de Cloud-provider?
- → Wat weet de ondernemer over het delen van data met derden?
- → Waar staat de data opgeslagen? En wat betekent dit voor de rechten?
- → Zet de ondernemer ook zijn kroonjuwelen in de cloud? Durft de ondernemer zijn meest geheime / gevoelige documenten in de cloud te zetten?
- → Heeft de ondernemer een plan als er geen internet is?
- → En wat gebeurt er als de cloud-provider niet te bereiken is?
- → Hoe houdt de ondernemer hackers buiten? Hanteert men een veilige wachtwoordenbeleid met 2FA/MFA? Doet men aan whitelisting, automatisch uitloggen, veilige verbinding (VPN)?
- → Hoe is het geregeld met backups (retentie, offsite, offline, restoretest)? Microsoft maakt zo goed als geen back-ups en geeft hooguit ‘best effort’-support als er iets mis is gegaan. Microsoft neemt enkel de verantwoordelijkheid over de beschikbaarheid van de infrastructuur (de datacentra, de servers, verbindingen, databases etc). De eindklant blijft eigenaar van de data en heeft daarmee ook de verantwoordelijkheid voor het bewaarbeleid ervan.
- → In de cloud is er vaak wel synchronisatie, een prullenbak en documentversies, maar dat zijn geen back-up maatregelen en de prullenbak gaat meestal maar 30 of 93 dagen terug. Als bij een synchronisatie een bestand verloren en versleuteld raakt, dan gebeurt dat ook aan de andere kant.
- → Weet de ondernemer wat er in de SLA staat over uptime garantie, veiligheidsmaatregelen, verantwoordelijkheid?
- → Synchronisatie: data komt hierdoor makkelijk buiten de de organisatie, bijvoorbeeld op mobiele telefoons en laptops. Hoe gaat de ondernemer hiermee om?
- → Accountbeheer, Rechten ingesteld op gegevens, wie beheert dit?
- → Zijn de koppelingen veilig en getest?
- → Weet de ondernemer heel zeker dat de cloud-provider betrouwbaar is?

Dit zien we in de praktijk...

- → Vaak wordt data uit de cloud gesynchroniseerd met lokale apparaten, zoals telefoons of laptops. Andersom wordt alles wat lokaal gebeurt met de cloud gesynct. Als iemand op zijn eigen apparaat per ongeluk een archief verwijdert of gijzelsoftware binnenhaalt, kan hij dit overbrengen naar de cloud en vanuit daar weer naar alle andere apparaten.
- → Doordat een medewerker per ongeluk malware op zijn eigen computer binnenhaalde, lukte het cybercriminelen toegang te krijgen tot de online boekhoudsoftware en Terminal Server. Ongemerkt wijzigden zij rekeningnummers van betalingen aan leveranciers in hun eigen bankrekeningnummer.

3. “Bij mij valt toch niets te halen”

Het gaat de crimineel niet om de absolute waarde van de spullen, maar om de waarde die ze voor de ondernemer hebben. Is hij bereid te betalen om gestolen of gegijzelde bestanden terug te krijgen? Criminelen volgen met dit verdienmodel de wet van de grote getallen: ze gooien heel veel hengeltjes tegelijk uit en zien wel waar en wanneer ze beet hebben. Ze mikken dus niet bewust op individuele ondernemers of bedrijven.

“Een cybercrimineel zoekt jouw bedrijf niet, maar hij het vindt het wel. Zeker als het makkelijk is om binnen te dringen, dan zal hij dit niet laten.”

Dit moet je weten over de miljoenen hackers die actief zijn:

- → Hackers kijken niet naar wie je bent of wat voor een bedrijf je hebt; ze scannen het hele internet af.
- → Massa is Kassa, veel kleine bedrijven hacken levert ook veel op.
- → Er is een verschuiving gaande van Corporate naar MKB en Privé, want daar valt nog veel te halen en de security is minder goed (minder budget geen IT afdeling).
- → Jouw data is wel interessant en kan verkocht of gegijzeld worden. In sommige gevallen komt het er op neer dat je losgeld moet betalen of stoppen met het bedrijf.
- → Jouw netwerk kan misbruikt worden voor andere activiteiten, zoals spam- en phishing, hacks op andere netwerk, cryptomining, botnet.
- → Voor een concurrent ben je misschien wel interessant.

Dit zien we in de praktijk...

- → Een architect bewaart zijn tekeningen in de cloud. Op die manier kan hij er altijd en overal bij. Toen hij per ongeluk op een phishing link klikte is er ransomware geïnstalleerd. De tekeningen hebben voor de cybercrimineel geen waarde, maar voor hem wel. Hij heeft een flink bedrag betaald om ze terug te krijgen.
- → Een tomatenkwekerij heeft een volledig geautomatiseerde kas. De controle over de systemen is overgenomen door criminelen die dreigen alle ph-waardes aan te passen. De tomaten hebben voor hen geen enkele waarde, maar de kweker moet snel handelen om zijn oogst te redden.
- → Een webshop is compleet afhankelijk van bereikbaarheid op internet. Hij wordt uit de lucht gehaald door een DDOS-aanval. De crimineel verdient er niets aan, maar de eigenaar ziet zijn gemiste omzet met de minuut oplopen en betaalt om de aanvallen te stoppen.

4. “Wij bewaren/verwerken geen persoonsgegevens”

Als onderneming heb je met verschillende partijen te maken. Zoals bijvoorbeeld klanten, leveranciers en personeel. Het is onwaarschijnlijk dat je nergens gegevens van hen bewaart. Denk hierbij aan NAW-gegevens, bankrekeningnummers, burgerservicenummers en kopie paspoorten. Zelfs de e-mailadressen van inschrijvers op de nieuwsbrief zijn al gegevens die je moet beschermen.

De feiten op een rij over persoonsgegevens:

1. Ieder bedrijf heeft data en persoonsgegevens, bijvoorbeeld van het personeel, klanten, leveranciers, financiële gegevens, bedrijfsgegevens, etc.
2. Soms valt er geen data te halen, maar een hacker kan er wel voor zorgen dat jouw bedrijf stil komt te staan
   en daardoor omzet misloopt. Denk aan het verstoren van productieprocessen, het platleggen van de webshop of het blokkeren van internet- of betalingsverkeer.
3. Jouw data, bedrijfsgeheimen etc zijn wel interessant voor jouzelf. Als je die kwijt bent door diefstal of door gijzeling, is dit een probleem voor de continuïteit van de onderneming.
4. Met een datalek van enkel NAW en e-mailadressen loop je al risico op een boete van de Autoriteit Persoonsgegevens.
5. Elke hack en ieder datalek brengt kosten met zich mee, geeft vertrouwensverlies en kost reputatieschade.

Dit zien we in de praktijk...

→ Een op het oog een onschuldig datalek kan ervoor zorgen dat via de onderneming persoonsgegevens op straat komen te liggen. Naast de reputatieschade die dit mogelijk oplevert, loopt het bedrijf ook het risico een boete van de Autoriteit Persoonsgegevens (AP) te krijgen.

→ Gehackte of gelekte gegevens van het bedrijf kunnen voor een crimineel net het ontbrekende puzzelstukje zijn om een plaatje compleet te maken. Vooral combinaties van bankrekening, creditcard, wachtwoorden, NAW-gegevens en geboortedatum zijn zeer interessant voor identiteitsfraude bijvoorbeeld.

→ Gehackte (of gelekte) gegevens worden doorverkocht aan andere criminelen. Er worden hele sites bijgehouden waar louche types voor een paar dollar data van anderen kunnen kopen.

Uitsmijter: enkele praktijkvoorbeelden van onze klanten (voordat ze klant bij ons werden uiteraard).

Door de jaren heen hebben onze cyber experts het nodige meegemaakt. Om een goed beeld te geven van hoe klanten in de maling werden genomen, of zelf steken hebben laten vallen, enkele illustratieve voorvallen. Uiteraard vond dit plaats voordat ze klant bij ons waren en besloten ze naar aanleiding van een incident om werk te maken van hun cyber security.

De irritante concurrent

Een van onze klanten verkoopt online tegoedbonnen (gamecards) voor computerspellen via een webshop. In Nederland zijn er maar twee grote spelers die deze producten online verkopen. Onze klant heeft te maken gehad met een DDoS aanval en hun webshop heeft er lange tijd uit gelegen. Via internet werden DDoS-as-a-Service platformen gebruikte voor de aanval. Voor enkele tientjes per maand werd de webshop continu bestookt met heel veel verkeer en daardoor onbereikbaar. Deze hacker deed dat in opdracht van de concurrent. Zij hebben dit aangegeven bij de politie en laten onderzoeken. De DDoS aanval was door een 16-jarige 'hacker' en een bekende van de concurrent, uitgevoerd.

Verdacht pakketje

Een tandartspraktijk heeft met een hack te maken gehad. In eerste instantie had hij het niet door, maar er was een bestelling gedaan van 20 iPhones via Bol.com. Deze werden een dag later bij hem op de praktijk afgeleverd. Nog geen halfuur later na de bezorging van het pakket stond er een busje voor zijn deur met drie kerels die deze bestelling bij hem op kwamen halen. Achteraf bleek dat zijn algemene mailbox gehackt was. In een van de mails stonden zijn inloggegevens van Bol.com opgeslagen.

Wat backuppen we ook alweer?

Tijdens onze scan gaan we diep in op het backup proces. Het backup proces moet goed op orde zijn want het is vaak een van de laatste redmiddelen bij een hack of ransomware. De meeste bedrijven maken wel back-ups van hun gegevens, maar de back-ups worden zeer zelden getest. Uit onze statistieken blijkt dat 6 op de 100 bedrijven hun back-ups regelmatig laat testen op een goede werking of op bijvoorbeeld versleuteling van ransomware. Een van onze klanten in de transportindustrie begon op ons advies om restoretestst te gaan doen. Door de restoretests kwam de klant erachter dat jarenlang iedere nacht back-ups gemaakt worden op de tapes. Maar deze back-ups zelf waren helemaal leeg. Ze bevatten dus geen bestanden. Door een configuratiefout werd alleen de mappenstructuur geback-upt, maar de inhoud van de mappen niet.

Perfect Day

Sparren of een afspraak maken?

Wij staan voor je klaar!

Contactgegevens

Caballero Fabriek Unit 70
Saturnusstraat 60
2516 AH Den Haag

E: contact@perfectday.nl
T: 085 048 61 09