
PERFECT DAY
CYBER ADVIES

UW CYBEREXPERT

Thomas Mes

thomas@perfectday.works

085-048 61 09

ALSTUBLIEFT,

Hier zijn de resultaten van de Cyber Scan. Het geeft u een goed beeld van de digitale veiligheid van Onderhoudsbedrijf Spaak. Complimenten, u heeft uw wetgeving goed op orde. Als het gaat om medewerker awareness adviseer ik u wel echt aan de slag te gaan. U doet dit snel en makkelijk door ons security pakket af te sluiten. Daarmee pakt u direct de meest voorkomende risico's aan.

De bevindingen en aanbevelingen in dit rapport zijn gebaseerd op de informatie die ik heb gekregen uit de afspraak op het kantoor van Robert Spaak op 1 januari 2020 en het telefonische overleg met Jos Brandt van ABC-IT.

Dit rapport beschrijft op hoofdlijnen de risico's in uw bedrijfsprocessen, gedrag van medewerkers en techniek. Het geeft ook weer in hoeverre u aan de wet- en regelgeving omtrent gegevensbescherming voldoet. U vindt per thema ook aanbevelingen en de uitwerking van hetgeen we besproken hebben.

Leest u het rustig door. Ik bel u binnen enkele dagen om te zien of u nog vragen heeft. Wilt u al eerder iets bespreken? Neem dan gerust contact met mij op!

CYBERADVIES

SCORE

U ziet hier de overall score van uw bedrijf per thema. De uitwerkingen en aanbevelingen per thema vindt u op de volgende pagina's.

MEDEWERKERS

Er is al enig cyberbewustzijn onder uw medewerkers, maar hier zijn verbeteringen mogelijk.

KRITIEK

TECHNIEK

Er is al heel wat dat goed geregeld is, maar kijk onder andere aandachtig naar de restoretests van uw back-up.

KAN BETER

WETGEVING

Uw AVG-administratie lijkt goed op orde te zijn. Houdt dit ook in de toekomst goed up-to-date.

GOED

NOODPROCES

De medewerkers weten wie ze intern kunnen aanspreken bij een hack of datalek, maar een echte procedure lijkt er niet te zijn.

ONVEILIG

ADVIES

ACTIELIJST

Hieronder volgt uw lijst met praktische actiepunten. Deze lijst is geordend van meest kritiek tot voor verbetering vatbaar.

TECHNIEK

Schakel de firewall in en houd uw firewall up-to-date.

KRITIEK: Een firewall in uw netwerk is de eerste lijn van verweer tegen aanvallen vanuit het internet op uw netwerk. Als er geen firewall aanwezig is of deze wordt niet up-to-date gehouden, is het risico groter dat u slachtoffer wordt van malware of een hack.

Er is een firewall aanwezig in uw netwerk op de router. Deze heeft u IT-beheerder destijds aangelegd, maar wordt niet door hem beheerd. Dat betekent dat firmware updates niet worden doorgevoerd op dit moment. Wij raden aan om iemand verantwoordelijk te maken voor het up-to-date houden van dit soort apparatuur.

TECHNIEK

Test het terugzetten van back-ups (restore tests).

KRITIEK: Worden back-ups niet op regelmatige basis getest? Dan weet u niet of het terugzetten wel goed werkt als de nood aan de man is.

Op dit moment worden er geen restore tests uitgevoerd om te testen of de back-up terug kan worden gezet. Wij adviseren om minimaal 1 keer per jaar een volledige restore test voor alle systemen uit te (laten) voeren. Het is verstandig om tussendoor ook af en toe een steekproef te doen door bijvoorbeeld een directory terug te zetten.

MEDEWERKERS

Stel een wachtwoordbeleid in.

ONVEILIG: Als u geen wachtwoordbeleid heeft, is de kans groot dat medewerkers voor meerdere accounts dezelfde wachtwoorden en/of zwakke wachtwoorden gebruiken. Als van één account de gegevens lekken, is het voor een crimineel eenvoudig om ook andere accounts binnen te dringen.

Wij adviseren om met medewerkers afspraken te maken over hoe ze met wachtwoorden om moeten gaan. Belangrijk daarbij is dat ze sterke wachtwoorden gebruiken en voor elk account een uniek wachtwoord (en dus ook geen wachtwoorden van privé accounts hergebruiken).
U kunt ook in de gaten houden of accounts van uw medewerkers op straat zijn komen te liggen. U kunt dit bijvoorbeeld doen via https://haveibeenpwned.com. Als dit het geval is, dan is het verstandig het wachtwoord van het betreffende account te wijzigen.

MEDEWERKERS

Gebruik een wachtwoordmanager.

ONVEILIG: Als u geen wachtwoordmanager gebruikt, is de kans groot dat u voor meerdere accounts dezelfde wachtwoorden en/of zwakke wachtwoorden gebruikt. Als van één account de gegevens lekken, is het voor een crimineel eenvoudig om ook andere accounts binnen te dringen.

Op dit moment heeft u een Excelbestand waarin u een lijst van wachtwoorden heeft staan, maar u kunt deze lijst beter in een wachtwoordmanager bewaren. Dit is een kluis waarin je alle wachtwoorden kunt opslaan en die ook integreert met bijvoorbeeld uw browser. U hoeft nog maar één wachtwoord te onthouden (het hoofdwachtwoord). In ons security pakket bieden wij een wachtwoordmanager aan.

MEDEWERKERS

Gebruik 2-factor authentication (2FA) waar dat mogelijk is.

ONVEILIG: Webservices en cloud-applicaties zijn vanaf elke plek toegankelijk. Bij het verlies van de inloggegevens is de kans groot dat derden in uw systeem kunnen komen. Dit risico kan verkleind worden door 2-factor authentication te gebruiken. Wanneer u 2-factor authentication gebruikt, heeft u voor het inloggen een zogenaamde 'tweede factor' nodig, vaak een bevestiging of een code op uw telefoon. Dit maakt het voor criminelen een stuk moeilijker om bij uw accounts te komen.

Goed om te zien dat er voor sommige systemen al 2-factor authenticatie wordt gebruikt. Wij raden aan om voor alle (kritieke) systemen die deze mogelijkheid bieden dit te gaan gebruiken. Denk hierbij aan het inloggen op de lokale server vanuit huis en het inloggen op de Exact Online.

TECHNIEK

Scheidt uw bedrijfs- en thuisomgeving.

ONVEILIG: Wanneer privé omgeving en bedrijfsomgeving niet goed gescheiden zijn, is het risico groter dat malware uw bedrijfsomgeving binnendringt. Een privécomputer wordt over het algemeen voor veel meer activiteiten gebruikt (bijvoorbeeld door andere gezinsleden) en daar is de kans een stuk groter dat er malware op terechtkomt.

Uw medewerkers kunnen thuis inloggen op de bedrijfsserver, zelfs op hun privécomputer. Wij raden aan om minimaal afspraken te maken met uw medewerkers over de beveiliging van hun eigen computer wanneer deze gebruikt wordt voor het werk. Beter is het om medewerkers die thuis mogen werken een laptop van de zaak mee te geven, die in beheer is van het bedrijf.

TECHNIEK

Beperk de rechten van uw medewerkers op hun apparaten.

ONVEILIG: Wanneer gebruikers rechten op hun apparatuur hebben die ze niet nodig hebben, dan kan dat de impact van bijvoorbeeld malware op uw systemen vergroten.

Uw medewerkers werken op dit moment met een local admin account op de computers. Dit is om praktische redenen gedaan. Desondanks raden wij aan om de rechten van medewerkers op hun computers te beperken. Laat ze in elk geval niet werken op een beheeraccount (zogenaamd admin account), maar op een gebruikersaccount met beperkte rechten. Als het niet nodig is dat medewerkers bijvoorbeeld zelf software installeren, beperk dit dan bijvoorbeeld.

MEDEWERKERS

Leg vast hoe medewerkers met bedrijfsdata omgaan.

ONVEILIG: Als medewerkers niet weten hoe ze met bedrijfsdata moeten omgaan, dan vullen ze dit naar eigen inzicht in. Vaak leidt dit tot onveilige handelingen bijvoorbeeld bij verzenden of opslaan van bestanden. Hiermee vergroot u de kans op een hack of datalek aanzienlijk. Maar liefst 90% van de cyber ongevallen is te herleiden naar menselijke fouten.

Wij raden aan om af te spreken (en vast te leggen in een document) hoe medewerkers met data moeten omgaan. Informeer uw medewerkers bijvoorbeeld in welke systemen welke data mag worden opgeslagen en dat er geen andere systemen mogen worden gebruikt (ook niet wanneer een klant er om vraagt). Leg bijvoorbeeld ook vast hoe (gevoelige) data met klanten wordt uitgewisseld.

TECHNIEK

Versleutel uw apparaten zoveel mogelijk.

ONVEILIG: Mocht uw telefoon of laptop gestolen worden en u heeft uw data niet versleuteld, dan liggen al uw gegevens op straat. Het is eenvoudig om bijvoorbeeld een onversleutelde harde schijf aan te sluiten op een computer en alle gegevens te kopiëren.

Wij adviseren om uw computers te versleutelen. Vooral voor de laptops aangezien deze regelmatig meegenomen worden. De meeste data wordt op de server opgeslagen, maar medewerkers zouden lokaal ook documenten kunnen opslaan. Als deze versleuteld zijn hoeft u zich geen zorgen te maken over eventuele (gevoelige) data die er wel of niet opstaat, mochten deze apparaten worden verloren of gestolen. Met Windows 10 Pro wordt standaard BitLocker meegeleverd waarmee u de harde schijf kunt versleutelen.

TECHNIEK

Zorg ervoor dat op afgedankte apparatuur geen bedrijfsgegevens meer staan.

KAN BETER: Regelmatig komen bedrijfsgegevens op straat te liggen omdat oude apparatuur niet goed is afgedankt. Dit geldt niet alleen voor computers, maar ook voor tablets en mobiele telefoons.

Goed dat u de harde schijven van uw apparatuur zelf vernietigt. Houdt ook de mobiele telefoons (en andere mobiele appratuur) in de gaten. Onze ervaring is dat deze makkelijker worden doorgegeven, bijvoorbeeld aan vrienden of kennissen. De mobiele telefoon moet dan minimaal teruggezet worden naar fabrieksinstellingen. Maak hierover ook afspraken met uw medewerkers, ook voor de privé telefoons waarop bedrijfsdata toegankelijk is.

MEDEWERKERS

Laat medewerkers hun computer vergrendelen.

KAN BETER: Een concurrent of crimineel zit binnen no time in uw bedrijfsgegevens of netwerk op het moment dat u een kop koffie gaat halen en uw computer onbeheerd achter laat.

Wij raden aan om alle computers (en ook telefoons) te voorzien van een automatische lock en medewerkers ook hun computers te laten locken wanneer zij weglopen van hun computer. Men loopt vrij makkelijk uw bedrijfsruimte binnen. De toetscombinatie Win + L lockt de computer en bij terugkomst is het even de muis bewegen of een toets indrukken, wachtwoord invoeren en de medewerker is weer in het systeem. Bijkomend voordeel: als u uw computer aan het einde van de werkdag vergeet af te sluiten, dan wordt deze automatisch gelockt.

NOODPROCEDURE

Zet een noodprocedure op papier.

KAN BETER: Als u geen gedocumenteerde noodprocedure heeft, is de kans groot dat medewerkers niet exact weten wat er moet gebeuren in het geval van een cyber incident. In alle hectiek kunnen fouten u dan duur komen te staan. Denk bijvoorbeeld aan het niet (tijdig) melden van een datalek of malware dat zich steeds verder verspreid.

Goed dat er een duidelijk intern aanspreekpunt is. Wij raden wel aan om een noodprocedure op papier te zetten met alle relevante telefoonnummers, zodat bij een hack gelijk inzichtelijk is wat er moet gebeuren. Zet hierin dan ook gelijk wat u moet doen bij een datalek. Een datalek hoeft u pas binnen 72 uur te melden, dus laat u even goed informeren door een jurist voordat u dit doet. Denk ook alvast na over of en zo ja wanneer u klanten gaat inlichten wanneer persoonsgegevens zijn gelekt.
Let er ook op dat medewerkers gestimuleerd worden om fouten te melden, bijvoorbeeld een klik op een link in een phishing mail. U wilt niet dat dit onder de pet wordt gehouden.

MEDEWERKERS

Leg de in - en uitdienstprocedure vast.

KAN BETER: Met enige regelmaat wordt er data gelekt door (boze) ex-medewerkers die toch nog in bedrijfssystemen konden of waarvan de sleutel niet was afgenomen. Vlak dit risico niet uit.

Wij raden aan om vast te leggen, bijvoorbeeld in een checklist, wat er allemaal moet gebeuren als iemand uit dienst treedt met daarin onder andere een overzicht van welke accounts moeten worden afgesloten. Dan is dit voor iedereen overzichtelijk en vergeet u niks en kan een andere medewerker het eventueel overnemen. Als u toch bezig bent neem dan gelijk ook op wat er moet gebeuren bij het in dienst treden en de toegangsrechten per functie voor de verschillende applicaties. Maak hier ook één iemand verantwoordelijk voor.

TECHNIEK

Wijzig het wachtwoord van de wifi regelmatig.

KAN BETER: Het wifiwachtwoord, vooral van een gastnetwerk, is vaak bij vele personen en apparaten bekend. Dit vergroot de kans dat het in handen komt van vreemden die u liever niet in uw netwerk heeft en die bijvoorbeeld illegale activiteiten via uw netwerk ontplooien. Hackers kopen vaak oude apparaten op. Niet vanwege de hardware, maar vanwege de gegevens en de wachtwoorden die er nog op staan.

Ons advies is om de wifiwachtwoorden regelmatig te wijzigen, minimaal 1 keer per jaar. Zeker voor de gastwifi, maar het is ook verstandig dit voor de bedrijfswifi te doen, hoewel de impact daarvan vaak groter is. Maak hier iemand verantwoordelijk voor en zet hiervoor op gezette tijden een reminder in de agenda van deze persoon. Maak ook het wachtwoord voor uw gastwifi sterker. Bezoekers typen dit toch vaak over van papier.

WETGEVING

Kijk nog even naar het contactformulier op uw website.

KAN BETER: De AVG schrijft voor dat u uw bezoekers en klanten informeert over uw verwerking van hun persoonsgegevens. Dit doet u bijvoorbeeld in een privacyverklaring. Als u uw klanten niet informeert kan de Autoriteit Persoonsgegevens u een boete opleggen.

U heeft op uw website een contactformulier staan. Ook is er een link naar de privacyverklaring in de footer. U kunt overwegen om in uw contactformulier een vinkje toevoegen waarin u expliciet toestemming vraagt aan de bezoeker voor de verwerking van zijn of haar persoonsgegevens om contact op te nemen met een link naar de privacyverklaring. Dan bent u helemaal compleet.

TECHNIEK

Stop met het gebruik van USB-sticks.

KAN BETER: USB-sticks kunnen al bij de fabrikant besmet zijn met malware. Zelfs als u de USB-stick formatteert voor gebruikt heeft u kans op besmetting met malware.

Goed dat u al zo min mogelijk gebruik maakt van USB-sticks. Spreek expliciet met uw medewerkers af dat zij niet zomaar USB-sticks van klanten of wie dan ook in hun apparatuur steken. U kunt ook overwegen om de USB-poorten dicht te zetten voor opslagmedia.

TECHNIEK

Controleer uw website op standaarden.

KAN BETER: Uw websitebezoekers lopen het risico gehackt te worden als u niet de meest actuele internetstandaarden toepast. Als zij bijvoorbeeld via een contactformulier op uw website gegevens naar u verzenden kunnen criminelen deze gegevens onderscheppen als deze niet (goed) versleuteld zijn.

Goed om te zien dat de website beschikbaar is via https en de http-versie ook wordt geredirect naar de beveiligde versie. Hts wordt echter niet ondersteund. Wij raden aan dit te gaan ondersteunen, vaak is dit vrij eenvoudig in te regelen door uw websitebouwer. Eventueel kunt u de hosting partij te vragen IPv6 en DNSSEC te gaan ondersteunen, maar dit heeft minder prioriteit wat ons betreft. Als laatste kunt u overwegen om security headers te gaan gebruiken op uw website, uw websitebouwer kan u hier meer over vertellen. U kunt zelf op https://internet.nl kijken of uw hosting partij het heeft geregeld.

WETGEVING

Houdt uw AVG-administratie up-to-date.

GOED: Voldoet u niet aan de AVG dan riskeert hiermee een boete van de Autoriteit Persoonsgegevens (AP). Deze boete kan oplopen tot 4% van uw jaaromzet. De AP kan al een onderzoek instellen naar aanleiding van een klacht van slechts 1 klant.

Het lijkt erop dat uw AVG-administratie goed op orde is. U heeft met alle partijen een verwerkingsovereenkomst afgesloten en een verwerkings- en incidentregister aangelegd. Wij raden aan om nog even na te gaan of alles up-to-date is. Laat de medewerker die ervoor verantwoordelijk is één keer per jaar weer even kijken of alles nog juist is.

ALGEMEEN

ORGANISATIE

Op 1 januari 2020 kwam ik bij u langs om de cybercheck uit te voeren. De organisatie zag er toen als volgt uit.

- Het bedrijf heeft ongeveer 17 medewerkers. Soms lopen er ook stagiaires rond, die ook toegang krijgen tot sommige systemen.
- Het IT-beheer is uitbesteed aan ABC-IT, maar Robert is het eerste interne aanspreekpunt als het om ICT gaat. IT-ondersteuning is op aanvraag, maar de IT-beheerder is één keer per maand op locatie aanwezig en controleert dan bijvoorbeeld ook de apparatuur. Lokaal staat een server en medewerkers werken op desktops. Een aantal medewerkers heeft een laptop en een mobiel van de zaak. Ook worden privé mobielen voor zakelijke mail gebruikt.
- Er wordt gewerkt met Windows 10 Pro en Office 365. Deze laatste wordt ook voor de mail gebruikt. De documenten worden op de server opgeslagen, maar kunnen ook lokaal op de computers staan. Als CRM-pakket wordt CRM-pro gebruikt, een webapplicatie. Voor de boekhouding wordt Exact Online gebruikt. De loonadministratie wordt gedaan door Loonport en staat ook bij deze partij. TeamViewer wordt gebruikt voor IT-ondersteuning op afstand.
- Naast contact- en NAW-gegevens worden er ook bankgegevens opgeslagen van klanten. Er is een personeelsadministratie aanwezig en deze staat op de eigen server.
- Het bedrijf is gevestigd in een verzamelpand waarin makkelijk bij elkaar naar binnen kan worden gelopen. De voordeur van het pand is open.