Veiligheid boven alles!

Cybersecurity checklist

- [ ] Medewerkers zijn bij ons verplicht om na minimaal 3 maanden hun **wachtwoorden te wijzigen** en er worden eisen gesteld aan de complexiteit van het gekozen wachtwoord.
- [ ] Mijn organisatie heeft een **datalekprotocol** opgesteld voor het geval er bedrijfsgevoelige en persoonsgevoelige informatie gelekt wordt.
- [ ] Onze organisatie maakt gebruik van **Multi Factor Authenticatie** (MFA) voor de toegang tot bedrijfsgegevens en samenwerkingstools.
- [ ] Bij onze organisatie is er een **beleid** voor het opslaan van bedrijfsgegevens.
- [ ] Het is bij onze organisatie mogelijk om **mobiele apparaten binnen de organisatie te beheren**. Bijvoorbeeld het op afstand wissen na verlies of diefstal.
- [ ] Onze medewerkers worden regelmatig **voorgelicht** over het herkennen en voorkomen van risico's op het gebied van cybersecurity.
- [ ] Al onze werkplekken zijn up-to-date en uitgerust met **minimaal Windows 10** en de laatste updates zijn gedaan aan software.
- [ ] Er zijn **firewalls** geïnstalleerd binnen ons netwerk en worden regelmatig voorzien van de nieuwste updates.
- [ ] Al onze werkplekken hebben up-to-date **antivirussoftware**.
- [ ] De bestaande **netwerkapparatuur** (switches, routers, AP's, e.d.) worden regelmatig gecontroleerd op **veiligheidsupdates**.
- [ ] Bij ons worden binnenkomende **e-mails gescand op bedreigingen en virusse**n.
- [ ] Bedrijfsktrische data wordt bij onze organisatie **encrypted** verwerkt en verstuurd.
- [ ] Onze organisatie beschikt over een **disaster recovery plan**.

valueIT

www.valueit.nl // office@valueit.nl // 040 257 5710

- [ ] Er worden bij ons regelmatig off-site **backups** gemaakt van onze digitale omgeving en data. Ook wordt er regelmatig een backup **restore test** uitgevoerd.
- [ ] Bij onze organisatie is er iemand aangewezen die verantwoordelijk is voor het **cybersecurity beleid**.
- [ ] Medewerkers hebben **geen toegang tot bedrijfsgegevens met privé apparaten** zoals eigen telefoons en laptops.
- [ ] Onze organisatie heeft een b**eleid omtrent in- en uit diensttredende medewerkers**. Denk hierbij aan verwijderen accounts, wijzigen wachtwoorden en toegankelijkheid tot applicaties en gegevens.
- [ ] Onze organisatie heeft een **goed SSL-certificaat**.
- [ ] Wordt het WiFi-wachtwoord **regelmatig** gewijzigd?
- [ ] Er wordt een **scheiding** gemaakt tussen het gasten-WiFi en de WiFi voor medewerkers.
- [ ] We maken gebruik van **netwerksegmentatie**.
- [ ] Werkplekken worden automatisch **gelocked** na een inactieve periode.
- [ ] Er is een **autorisatiematrix** aanwezig waarin staat beschreven wie toegang heeft tot welke gegevens en applicaties.
- [ ] Onze organisatie beschikt over een up-to-date **configuration management database** (CMDB) waarin wordt bijgehouden welke hard- en software er actief is binnen de organisatie.
- [ ] **Internetgebruik wordt gemonitord**.
- [ ] Alleen met een **VPN verbinding** kan men op afstand toegang krijgen tot bedrijfsgegevens.
- [ ] Wachtwoorden en accounts worden niet gedeeld in onze organisatie. Iedereen heeft een **eigen account** voor software en portals.
- [ ] Er vindt actieve **monitoring** plaats op ICT-infrastructuur.

valueIT

www.valueit.nl // office@valueit.nl // 040 257 5710

Op volgorde van de checkpoints

Uitleg

Wachtwoorden

Het belang van een goed wachtwoord kan niet vaak genoeg benoemd worden. Cybercriminelen beschikken over lijsten met miljarden wachtwoorden, die zijn buitgemaakt op verschillende websites. Hoe langer je een wachtwoord gebruikt hoe groter de kans dat het op deze lijst komt. Ook maken cybercriminelen gebruik van geavanceerde software om wachtwoorden te kraken. Hoe eenvoudiger het wachtwoord hoe sneller het is te kraken. Dus zorg dat je medewerkers om de drie maanden het wachtwoord moeten wijzigen en eisen stelt aan de complexiteit.

Datalekprotocol

Een datalek is het opzettelijk of onopzettelijk vrijgeven van beveiligde informatie aan een onvertrouwd publiek. In Nederland moet je datalekken melden. Doe je dat niet op tijd en adequaat, dan kan dit leiden tot fikse boetes. Dus zorg voor een datalekprotocol. Een AVG-compliant document waarin de procedure staat beschreven die je organisatie moet volgen wanneer er persoonsgegevens zijn gelekt, kwijtgeraakt, gestolen of op andere wijze in verkeerde handen zijn gekomen.

MFA

Kort samengevat is Multi-Factor Authenticatie (MFA) een authenticatie methode waarbij de onlinegebruiker meerdere stappen succesvol moet doorlopen om ergens toegang tot te krijgen. MFA is de 'opvolger' van 2FA en is steeds meer de overkoepelende term geworden. Dus zorg voor MFA binnen de organisatie en zorg voor een betere beveiliging, een vereenvoudiging van de aanmeldprocedure (jazeker, vereenvoudiging) en een stap richting AVG conformiteit.

Beleid

In het kader van de AVG en GDPR is het van belang om altijd te weten waar je data zich bevindt en er controle over te houden. Door veel mobiele apparaten en mobiele gegevens dragers (USS-sticks) is het steeds moelijker om je data onder controle te houden. Dus een beleid is onmisbaar en neem daarin concreet regels in op omtrent het opslaan van bedrijfsgegevens, zodat je medewerkers weten wat wel en niet toegestaan is met jullie bedrijfsgegevens.

Mobile device management

Meer mobiele apparaten = meer risico in de organisatie. Mobiele apparaten kunnen kwijtraken, gestolen worden of gebruikt worden door ongeautoriseerde personen. Is dat het geval, dan kun je met Mobile Device Management laptops, telefoons of tablets op afstand locken en wissen. Maar ook voor beheerwerkzaamheden is MDM van belang, zo kun je mobiele apparaten van buitendienst medewerkers direct updaten in geval van noodzakelijke beveiligingsupdates.

Voorlichting

80 procent van de beveiligingrisico's ontstaat door menselijk handelen. Vaak is er totaal geen kwade opzet in het spel maar hebben mensen gewoon geen besef van de risico's van hun acties.
Het regelmatig voorlichten van je medewerkers over het herkennen en voorkomen van cybersecurity risico's is dan ook van enorm belang.

Windows 10
Windows 10 is het enige Operating System dat nog volledig ondersteund wordt door Microsoft. Voor alle oudere OS worden geen beveiligingsupdates meer uitgebracht. Het gebruik van Windows XP, Vista, 7 of 8 binnen je bedrijf is gevaarlijk en een absolute no go. Ook als deze oudere OS alleen wordt gebruikt om in te loggen op een remote werkplek is dit nog steeds gevaarlijk. Dus zorg dat je systemen de laatste operating systems bevatten.

Firewalls
Een firewall is een device dat de systemen binnen een netwerk of computer kan beschermen tegen misbruik van buitenaf als een soort digitale poortwachter. Een firewall staat tussen een computer en het verbindingspunt met een extern netwerk of het internet. Hij besluit welk netwerkverkeer verder mag komen en welk verkeer als gevaarlijk wordt beschouwd. In wezen onderscheidt een firewall het goede van het slechte, het betrouwbare van het onbetrouwbare. Een noodzakelijkheid voor iedere organisatie dus.

Antivirussoftware
Antivirussoftware scant bestanden om te zoeken naar virussen die overeenkomen met een lijst van bekende virussen. Ook identificeren ze verdacht gedrag door computerprogramma's, wat op een besmetting kan wijzen. Dankzij updates blijft je antivirussoftware veilig en stabiel draaien. Als dergelijke updates niet plaatsvinden, is je apparaat een makkelijker doelwit voor virussen, malware en spyware. Daarnaast kan een niet-geüpdatete computer misbruikt worden voor cyveraanvallen of het versturen van spam.

Netwerkapparatuur
Dat je computer regelmatig updates nodig heeft is inmiddels wel algemeen bekend maar dat ook al je netwerk apparaten geregeld een update nodig hebben is minder bekend. De netwerkapparatuur zijn vaak de eerste obstakels die cybercriminelen tegenkomen, mochten hier beveiligingslekken aanwezig zijn, worden ze een eenvoudige prooi.

E-mailscans
Veel gebruikers denken ten onrechte dat de antivirussoftware ook automatisch je emailverkeer scant, echter is dit vaak niet het geval. Je zult hier dus dezelfde aandacht aan moeten besteden als aan je antivirussoftware aangezien 90 % van de besmettingen plaats vindt via email.

Encryptie
Encryptie is het basisbestanddeel van gegevensbeveiliging. Het is de eenvoudigste en belangrijkste manier om te voorkomen dat informatie van een computersysteem wordt gestolen en gelezen door iemand met malafide intenties.

Disaster Recovery Plan
Een disaster recovery plan is een document dat beschrijft hoe een organisatie haar business zo snel mogelijk weer kan hervatten na een calamiteit. Het beschrijft bijvoorbeeld het stappenplan nadat je slachtoffer bent geworden van ransomware.

Backups
Gebruik goede backup software en maak backups buiten je netwerk, bijvoorbeeld in de Cloud. Dit klinkt eenvoudig maar dat is het helaas niet. Het doel van cybercriminelen is namelijk niet alleen het versleutelen van je bestanden maar ook het versleutelen van je backup, op deze manier kun je namelijk niets herstellen uit je back-up. Met gedegen backup in de cloud voorkom je dat deze backup wordt geïnfecteerd en kun je vanuit deze back-up snel je bestanden herstellen. Ook is het van belang regelmatig te testen hoe je back-up procedure functioneert. Niets zo vervelend om erachter te komen dat je backups niet bruikbaar zijn als je net slachtoffer bent geworden van een ransomware aanval.

Cybersecurity beleid
Een Information of Cyber Security Officer is binnen de organisatie verantwoordelijk voor het opstellen van al het beleid en procedures omtrent (cyber)security. Dit kan gaan van in/uit dienst procedures van medewerkers tot het opstellen van beleid op het gebied van patch management. Het is van belang dat binnen iedere organistie iemand wordt aangewezen die hier verantwoordelijk voor is. Je kunt eigenlijk niet meer zonder.

Privé apparaten beleid
Als medewerkers met een privé apparaat inloggen op het bedrijfsnetwerk heb je vaak geen controle over geïnstalleerde software en veiligheid. De virtuele werkplekken kunnen helemaal up-to-date zijn, maar als de apparatuur van de eindgebruiker verouderde software heeft, bent je alsnog kwetsbaar. Als organisatie heb je geen controle over updates en ouderdom van het OS van de computer van de medewerkers. Daarnaast heb je geen controle over antivirussoftware op het device.
Door de crisisomstandigheden is sprake van een verlaagd veiligheidsbewustzijn en door de fysieke afstand worden medewerkers lakser met het vragen om hulp en het melden van potentiële incidenten. Daarnaast nemen aanvalsoppervlakken toe nu iedereen thuiswerkt.

In- en uitdienst beleid
Wanneer iemand in dienst komt, worden er voor de nieuwe medewerker allerlei accounts aangemaakt, toegangscodes uitgereikt, sleutels, laptop, telefoon, etc, uitgedeeld. Het is van groot belang om hiervoor een goede administratie te voeren. Doe je dit niet, dan is het onmogelijk om nog te achterhalen wat de medewerker allemaal moet inleveren bij vertrek en misschien nog wel belangrijker: welke accounts moeten worden afgesloten om te voorkomen dat de medewerker nog toegang heeft tot bedrijfsgegevens.

SSL-certificaat
Een SSL-certificaat is een bestand dat zorgt voor een betere beveiliging van gegevens tussen de server (van jouw website) en een internetbrowser (zoals Chrome of Internet Explorer). Zo beveilig je login- en betalingsgegevens.

Persoonlijke WiFi wachtwoorden
Bij veel bedrijven zie je dat er één wachtwoord wordt gehanteerd voor toegang tot het bedrijf-WIFI. Dit levert in veel gevallen behoorlijke risico's op. Iedere keer dat een medewerker uit dienst treedt moet het WIFI-wachtwoord worden gewijzigd voor heel de organisatie, gebeurt dit niet heb je een security breach, doe je dit wel krijg je problemen met alle andere devices die met je WIFI verbonden zijn. Het is dus beter om per gebruiker een persoonlijk WIFI-wachtwoord te gebruiken zodat je niet in de problemen komt wanneer er iemand uit dienst gaat.

WiFi scheiding
Een absolute no go is het toestaan van gasten op je algemene WiFi. Op deze manier hebben al je gasten toegang tot de bedrijfsgegevens op je Netwerk. Stel altijd een apart WiFi kanaal ter beschikking voor je gasten, maar geef gasten nooit toegang tot je algemene WiFi.

Netwerksegmentatie
Netwerksegmententatie is het aanbrengen van virtuele groepen in het computernetwerk. Het verkeer tussen deze 'virtuele netwerken' controleer of blokkeer je met behulp van een firewall. Met als doel om een incident op te sluiten in een deel van het netwerk, zodat andere delen ongeschonden blijven. Het digitale equivalent dus van branddeuren. Netwerksegmentatie is een belangrijk instrument om te voorkomen dat een cyberaanval je hele netwerk platlegt. Een segmentatieproject kan vrij complex zijn, maar het resultaat na afronding is absoluut de moeite waard.

Locken van werkplekken
Een medewerker die zijn computer onbeheerd en niet gelocked achterlaat kan leiden tot een datalek. Vandaar dat het van belang is dat computers automatisch op slot gaan na een inactieve periode van bijvoorbeeld 5 minuten.

Autorisatiematrix
Met een autorisatiematrix regel je de toegangsrechten. Oftewel: wie heeft toegang tot welke informatie en vanaf welk device? Bijna alle organisaties werken met persoonsgegevens. Denk maar aan je personeelsadministratie of klantenbestanden. Hierin staan bijvoorbeeld namen, (e-mail) adressen en telefoonnummers. Door de AVG is het voor organisaties nog belangrijker geworden om te verantwoorden welke gegevens ze verwerken. Daarnaast moeten ze aangeven waarom ze dat doen en hoe de data wordt beveiligd. Autorisatiebeheer is daarbij onmisbaar. Met een goede autorisatiematrix behoud je het overzicht en voorkom je datalekken en eventuele boetes.

CMDB (configuration management database)
Een CMDB is een centrale database van alle hardware- en softwareactiva die vragen beantwoordt als: Welke soorten hardware heeft de organisatie? Wat is het exacte gebruik van een bepaalde softwarelicentie? Hoeveel versies zijn er van een software? Welke middelen worden toegewezen aan gebruikers die de organisatie hebben verlaten?
Een organisatie heeft de kenmerken van een organische entiteit, het groeit en is zeer complex. Met de groei wordt de IT-infrastructuur ook een uitdaging om bij te houden.
Door een register bij te houden van wie wat bezit en de problemen waarmee elk activum wordt geconfronteerd, en door een risicobeoordeling te doen door een duidelijk beeld te geven van het gebruik van licenties, maakt een CMDB het leven van IT-beheerders een stuk eenvoudiger**.**

Internetgebruik monitoren
Het monitoren van internetgebruik is van belang omdat cybercriminelen steeds vaker gebruikmaken van frauduleuze websites en website-links om systemen te infecteren.

VPN

Met een VPN (Virtual Private Network) leg je een beveiligde verbinding tussen jouw zakelijke apparaten (computer, tablet en smartphone) en het internet. Zo ben je afgeschermd online. Handig bijvoorbeeld als je veilig gebruik wilt maken van een openbaar wifi-netwerk als je buiten het kantoor online moet en verbinding moet maken met de servers van je bedrijf.

Wachtwoorden delen

Dit lijkt een no-brainer maar vaak zie je dat uit praktische- of kostenoverwegingen toch accounts worden gedeeld door collega's. Zorg voor een beleid wat dit niet toestaat en met gebruik van een goede autorisatiematrix breng je in kaart wie toegang heeft tot welke informatie en vanaf welke devices.

Locken van werkplekken

Een medewerker die zijn computer onbeheerd en niet gelocked achterlaat kan leiden tot een datalek. Vandaar dat het van belang is dat computers automatisch op slot gaan na een inactieve periode van bijvoorbeeld 5 minuten.

Monitoring op ICT-infrastructuur

De performance van uw systemen is belangrijk. Door deze goed te monitoren, zorgt u ervoor dat kritieke services een maximale uptime hebben. Door het proactief monitoren van uw netwerk worden grote storingen voorkomen en wordt uitval van de apparatuur tot een minimum beperkt.