CYBERSECURITY

IS UW BEDRIJF CYBERPROOF?

BELANGRIJKSTE RISICO'S DIE WIJ ZIEN

→ №1 Eigen werknemers die procedures m.b.t. cybersecurity niet in acht nemen

→ №2 Gegevens die vanuit uw systemen worden gehaald en hackers mee aan de slag gaan

→ №3 Grote schade/ernstige verstoring van de bedrijfsvoering door een hack

→ №4 Imagoschade

Hoe gaat u hier iets tegen doen?

Wij geven u enkele tips.

INLEIDING

Cyberaanvallen, hackers, u leest er dagelijks over in de krant. Het kan u ook overkomen want het is de snelst groeiende vorm van criminaliteit. Ruim 60% van het MKB heeft te maken met cybercrime. De schade hiervan voor de maatschappij bedraagt jaarlijks 10 miljard euro, en het aantal cyberaanvallen in 2016 is al zes keer hoger dan in 2013. Bij Cybercrime kunt u denken aan: ransomware, cryptoware, malware, hacking, phishing, fraude en oplichting.

Weet u hoe u zich hier zo goed mogelijk tegen kunt beschermen? Is uw bedrijf cyberproof?

AAN BOD KOMT:

- Tips voor een betere cybersecurity en informatie over de beveiliging van persoonsgegevens;
- Algemene informatie omtrent cybersecurity en de meldplicht datalekken;
- Cybersecuritybeeld Nederland 2017

TIPS DIE U SNEL KUNT TOEPASSEN INZAKE CYBERSECURITY

Gezien de verschillen tussen de bedrijven/organisaties en de diversiteit en omvang van het onderwerp is geen one-size-fits-all benadering mogelijk. Desalniettemin hebben wij op basis van informatie van IT-Bedrijven enkele tips voor u:

1_____

Inventariseer welke data belangrijk voor u of voor uw klanten zijn. Maak hiervan een verwerkingsregister (wie is verantwoordelijk, waar is het opgeslagen, wanneer moet het worden verwijderd). Vraag niet meer gegevens aan medewerkers en cursisten dan nodig (dataminimalisatie).

2_____

Deel niet meer gegevens dan nodig met uw partners en bespreek of uw zakenpartners de beveiliging op orde hebben alvorens u data deelt (vraag bijvoorbeeld of ze externe expertise inhuren en wie dan?). Zorg voor een goede bewerkingsovereenkomst.

3_____

Maak wachtwoorden veranderen verplicht. Stel ook hoge eisen aan wachtwoorden. Of nog beter maak een gelaagde vorm van beveiliging. Pas “twee-staps-verificatie” voor uw medewerkers en cursisten toe (wachtwoord + mobiele telefoon, zoals bij banken).

4_____

Maak regelmatig een back-up van de (belangrijke) data en test ook periodiek of de back-up werkt en compleet is. Bewaar de back-up tot 180 dagen terug omdat u soms pas na 90 dagen of later de hack ontdekt.

5_____

Verwijder op tijd data. Alle data die u niet heeft, kunt u ook niet lekken.

6_____

Pas toegangsbeperking toe, denk ook aan ZZP'ers en stagiairs. Blokkeer de toegang voor oud- medewerkers.

7_____

Pas op met shared hosting. De kosten zijn lager, maar vergewis u ervan dat de beveiliging van de andere websites ook tenminste even goed is als uw website.

8_____

Overweeg samenwerking/kennis delen op het gebied van cybersecurity. Dit kan de kosten drukken.

9_____

Maak en oefen een cybersecuritycalamiteitenplan (bestaande uit: draaiboek, communicatieplan en ICT-inbraakoefening).

10____

Ontwikkel kennis en expertise bij medewerkers op het gebied van cybersecurity. Veel incidenten worden door werknemers ontdekt.

11____

Overweeg of een cybersecurity dekking bij een verzekeraar voor u interessant is.

12____

Schakel een deskundige in. Neem contact op met de NRTO voor welke deskundige u kunt inschakelen tegen een gereduceerd tarief.

ALGEMENE INFORMATIE OVER CYBERSECURITY EN DE MELDPLICHT DATALEKKEN

Aan bod komt:

- WAT ZIJN CYBERSECURITY EN CYBERCRIME?
- BELANG VAN CYBERSECURITY
- WIE IS VERANTWOORDELIJK VOOR CYBERSECURITY
- WERKEN IN DE CLOUD
- CYBERSECURITY EN PRIVACYWETGEVING
- DE MELDPLICHT DATALEKKEN.

WAT ZIJN CYBERSECURITY EN CYBERCRIME?

Cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT door derden. Cybercrime is een vorm van criminaliteit gericht op een ICT-systeem of de informatie die door ICT wordt verwerkt. Een digitale aanval is een reeks handelingen die inbreuk maakt op informatiesystemen, waarbij de beschikbaarheid, integriteit of vertrouwelijkheid van de informatie wordt aangetast.

BELANG VAN CYBERSECURITY

Cybersecurity is een randvoorwaarde voor het goed functioneren van uw bedrijf. Online leren kan geblokkeerd worden met een hack. Naast de omzetschade heeft u reputatieschade en schade om weer back in business te komen (waaronder dure ICT consultants). Het belang van cybersecurity lijkt alleen maar groter te worden omdat steeds meer bedrijven afhankelijk zijn van ICT systemen. Bij onderwerpen die cybersecurity raken, spelen individuele, organisatorische, keten- en maatschappelijke belangen, die soms tegenstrijdig kunnen zijn. De toename van de afhankelijkheid van de Nederlandse samenleving van ICT en het belang van cybersecurity gaan hand in hand. Voorheen waren banken vaak het doelwit van hackers. Nu banken steeds meer zijn gaan werken aan hun ‘ digitale superkluis’ zoeken hackers ook steeds meer andere sectoren waaronder mogelijk onderwijsinstellingen aldus FOX-IT.

WIE IS VERANTWOORDELIJK VOOR CYBERSECURITY?

Elk bedrijf heeft zorgplichten op het terrein van cybersecurity. Deze zorgplicht heeft u bijvoorbeeld richting cursisten of werknemers. Bij kleinere bedrijven, zoals bij de meeste NRTO leden, ligt de verantwoordelijkheid bij de directeur. Bij grote opleiders is het bestuur/de directie van het bedrijf verantwoordelijk voor cybersecurity. Binnen het bestuur /de directie moet duidelijk zijn wie hierbij het voortouw neemt. U kunt hierover meer informatie vinden in de door de Cyber Security Raad eerder uitgegeven ‘Cyber security guide for boardroom members’. Het is daarom noodzakelijk om cybersecurity op de agenda van het bestuur/de directie te plaatsen.

WERKEN IN DE CLOUD?

Als ik werk in de Cloud ‘moet’ ik dit document dan ook lezen? Ook werken in de Cloud is niet 100 procent veilig. Voor MKB bedrijven is werken in de Cloud desalniettemin vaak wel een goede oplossing, omdat een eigen ICT afdeling met voldoende actuele kennis te kostbaar is. Goede cloudleveranciers voeren software updates uit en zijn over het algemeen ook goed beveiligd. Kies bij voorkeur voor een cloudleverancier in de EU. De privacywetgeving stelt namelijk hoge eisen aan de doorgifte van persoonsgegevens naar landen buiten de Europese Unie. Meer informatie hierover klik HIER. Lees ook eens de voor- en nadelen over het werken in de Cloud in dit artikel. Het artikel is gedateerd maar is nog steeds toepasbaar.

CYBERSECURITY EN PRIVACYWETGEVING

Natuurlijk is er een link tussen cybersecurity en privacywetgeving. Wij hebben het onderwerp wel gesplitst in de servicedocumenten. Er is ook een servicedocument privacywetgeving beschikbaar. Deze kunt u vinden door in te loggen op de NRTO website (ledenlogin). Cybersecurity maatregelen neemt u ook om persoonsgegevens van uw studenten te beschermen. Ook in de juridische documenten, zoals bewerkingsovereenkomsten en mogelijk ook in algemene voorwaarden, staan soms bepalingen opgenomen over cybersecurity.

DE MELDPLICHT DATALEKKEN

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Per 1 januari 2016 is de meldplicht datalekken ingevoerd. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Organisaties die een datalek willen melden bij de Autoriteit Persoonsgegevens kunnen dat doen via het meldloket datalekken. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, IPad of telefoon een inbraak in een databestand door een hacker.

De Autoriteit Persoonsgegevens kan bij overtreding van de meldplicht datalekken hoge boetes opleggen. Op de website van de Autoriteit Persoonsgegevens vindt u uitgebreide informatie, zie Meldplicht datalekken. Zie ook de Beleidsregels-meldplichtdatalekken.

BIJLAGE

BIJ DE VOLGENDE TIPS VERWIJZEN WIJ U DOOR NAAR VERSCHILLENDE WEBSITES WAAR MEER INFORMATIE STAAT

1 ° Cybersave Yourself is de beveiligingscampagne voor onderwijs en onderzoek. Lees de tips van op de website Klik HIER. Laat uw werknemers ook de game spelen van Cybersave Yourself. Klik HIER.

2 ° Lees het document Cybercrisisoefening. Dit document is gericht op de onderwijssector. Klik HIER.

3 ° Volg de adviezen van het Nationaal Cyber Security Centrum (NCSC).

4 ° De Veilig Zakelijk Internetten Academy helpt u om te bepalen waar u aandacht aan moet besteden om veilig online zaken te kunnen doen. Dit is een initiatief van MKB-Nederland en VNO-NCW. U kunt ook de kwetsbaarheid van uw eigen website in dit project testen.

5 ° Het nieuwe Digital Trust Center (DTC) zal ook relevante informatie voor het MKB publiceren. Bezoek de website medio 2018 eens. In september 2017 heeft het kabinet aangegeven geld vrij te maken om het DTC te lanceren. Begin 2018 gaat het DTC van start.

6 ° De handreiking van de Cyber Security Raad (CSR) voor bedrijven op het gebied van cybersecurity kunt u doornemen. Hier kunt u de handreiking met checklisten downloaden. Goed en praktisch document.

7 ° De CSR heeft meer informatie dan alleen de handreiking. De publicaties kunt u HIER vinden. Met name de speciale uitgave van het magazine uit maart 2017 is interessant. Daarin leest u vooral het belang van een goede cybersecurity.

8 ° De International Chamber of Commerce: heeft ook een uitgave voor bedrijven, de: “Cyber Security Guide for Business, waarin concrete handvatten voor bedrijven ter voorkoming van cybercriminaliteit staan. Wel is de informatie al enigszins gedateerd (2015). Download hier uw exemplaar van de ICC Cyber Security Guide for Business.

9 ° Een interessante website voor leden die meer willen lezen over cybersecurity is die van The Hague Security Delta (HSD) , the leading security cluster in Europe.

10 ° De Autoriteit Persoonsgegevens (AP) heeft in het verleden richtsnoeren opgesteld die uitleggen hoe de AP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de 'oude Wbp' toepast. Hoewel de Wbp per eind mei 2018 niet meer van toepassing is, kunt u dit document wel gebruiken als richtsnoer. Lees hier deze richtsnoeren*.

Een korte passage (samengevat) en een illustratie (vorige pagina) die wij graag met u delen:

CYBERSECURITYBEELD NEDERLAND 2017:

DIGITALE WEERBAARHEID NEDERLAND BLIJFT ACHTER OP GROEIENDE DREIGING

De digitale weerbaarheid in Nederland blijft achter bij de groei van dreigingen. Overheid, bedrijfsleven en burgers nemen veel stappen om de digitale weerbaarheid te vergroten, maar dit gaat niet snel genoeg. Dat blijkt uit het Cybersecuritybeeld Nederland 2017 (CSBN 2017) dat demissionair staatssecretaris Dijkhoff naar de Tweede Kamer heeft gestuurd.

Dijkhoff:

" Het besef van investeren in cybersecurity groeit in Nederland in de gehele maatschappij. Toch moeten we blijven investeren in kennis en kunde om als Nederland op topniveau te blijven. Daarom spreken we met het bedrijfsleven, het onderwijsveld en vertegenwoordigers uit vitale sectoren. We moeten samenwerken om Nederland digitaal veilig te houden. Dit cybersecuritybeeld bevestigt dat iedereen n odig is om de snel digitaliserende wereld veilig te houden. Bedrijven door bijvoorbeeld geld te reserveren om hun netwerk veilig te houden, gewone Nederlanders door digitaal veilige spullen te kopen. "

Net als vorig jaar blijft cybercriminaliteit een belangrijk punt van aandacht. Cyberaanvallen zijn aantrekkelijk vanwege de grote impact door inzet van vrij beperkte middelen en raken de gehele samenleving. Ook houdt de dreiging van statelijke actoren aan, meer dan honderd landen spioneren wereldwijd met digitale middelen en gebruiken digitale aanvallen om democratische processen te beïnvloeden.

De ontwikkeling van internet of things brengt naast kansen ook veel risico's met zich mee. Veel apparaten bevatten kwetsbaarheden waarvoor geen beveiligingsupdates uitkomen. Op die manier kunnen deze apparaten worden misbruikt voor bijvoorbeeld DDoS-aanvallen. Ook de sterke afhankelijkheid van een beperkt aantal buitenlandse aanbieders van infrastructuurdiensten brengt risico's met zich mee. Hoewel grote leveranciers zich beter tegen aanvallen kunnen wapenen, zorgt de afhankelijkheid ervan voor grote impact als zij wel geraakt worden. Volgens Dijkhoff laten de bevindingen uit het CSBN zien dat er de komende jaren geïnvesteerd moet blijven worden om de digitale weerbaarheid van Nederland te vergroten.

Dijkhoff:

“ De afgelopen jaren is er structureel meer geld vrijgemaakt in de begroting van Veiligheid en Justitie om de Nederlandse cybersecurity te versterken. Daarbij zijn bijvoorbeeld de publiek private samenwerking versterkt en de aanpak van cybercrime en detectie van digitale dreigingen geïntensiveerd. Gezien het zorgelijke beeld van 2017 blijven deze acties en investeringen broodnodig.”

Bron: Bekijk de CSBN-animatie op: Youtube. Rapport dat de moeite zeker waard is om te lezen: Cybersecuritybeeld Nederland 2017.

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)