VRAAG & ANTWOORD CYBERCRIME

Wat is veiliger, digitale of fysieke back-up?
De term back-up wordt gebruikt voor 2 varianten. De bestandskopie en systeemkopie. Een bestandskopie kopieert alleen je bestanden, geen applicaties of systemen. Een systeemkopie is een één-op-één kopie van de complete harde schijf van je computer. Wanneer er iets mis gaat kan deze kopie geraadpleegd worden om bestanden, instellingen en programma's te herstellen. Maak de back-up op zowel een fysieke als digitale locatie, dat is het veiligste. Maak de back-up daarnaast dagelijks en test regelmatig of een back-up werkt. Kijk voor meer informatie op https://www.digitaltrustcenter.nl/goede-backup

Wat moet je meenemen/veilig stellen voor de aangifte?
Neem altijd contact op met de politie via 0900-8844 of kijk op https://www.politie.nl/onderwerpen/cybercrime.html, de politie kan je vervolgens verder helpen.

Hoe kan ik mijn werknemers weerbaarder maken tegen cybercrime aanvallen?
Blijf benadrukken dat uw werknemers zelf ook mee kunnen werken aan de digitale veiligheid van uw bedrijf. Dit zit al in kleine, simpele dingen zoals:

- Gebruik een lang wachtwoord (bijvoorbeeld wachtwoordzinnen).
- Denk na voordat je klikt, open geen bestanden van onbekende afzenders.
- Steek niet zomaar onbekende USB-sticks in de computer.
- Laat wachtwoorden niet slingeren en verander ze regelmatig.
- Update alle apparaten, zeker als dit niet automatisch gaat i.v.m. bijvoorbeeld thuiswerken.
- Zorg voor een open cultuur waarbij werknemers gemakkelijk en snel richting leiding/ICT kunnen afstappen bij elke vorm van twijfel.
- Zorg voor tweestapsverificatie.

Kijk voor meer tips op: https://www.vno-ncw.nl/forum/cybersecurity-zo-wordt-je-bedrijf-veilig-6-stappen

Hoe weet ik dat ik gehackt ben?
Tekenen dat u gehackt bent: geen toegang meer tot het apparaat of bestanden, opduiken van nieuwe software of programma's die u niet herkend, berichten van hackers met losgeld eis, de computer werkt zonder interne input (de muiscursor gaat uit zichzelf bewegen bijvoorbeeld), mensen ontvangen berichten vanuit uw bedrijf die niet vanuit u verzonden zijn.

Kijk ook eens op https://haveibeenpwned.com/ om te checken of u eerder slachtoffer bent geweest van een datalek waardoor gegevens op straat zijn komen te liggen.

Wat moet ik doen als mijn bedrijf gehackt is?
Ga dan snel naar https://www.hackhelpdesk.nl/

Ik heb wel eens iets gehoord over een Incident Response Plan. Wat is dit en heb ik dit nodig?
Incident response is het proces waarmee een organisatie omgaat met een incident en de gevolgen van een incident. Het is raadzaam om een plan te hebben zodat er gecoördineerd actie genomen kan worden wanneer een incident plaatsvindt: een Incident Response Plan. Een incident response plan kan worden omschreven als een set instructies om medewerkers te helpen om beveiligingsincidenten te detecteren, hierop te reageren en mogelijke schade te herstellen. Bijvoorbeeld in het geval van een verstoring, een datalek of een digitale aanval. Het doel is om snel, kalm en adequaat te kunnen reageren om schade te beperken en herstelwerkzaamheden te minimaliseren. Meer informatie: https://www.digitaltrustcenter.nl/informatie-advies/incident-response-plan

Welke risico's zijn groter geworden door het vele thuiswerken en hoe kan ik die beperken?
Thuiswerken brengt verschillende risico's met zich mee, zoals onveilige wifi en onveilig mailverkeer. Meer info: https://www.mkb.nl/forum/de-6-grootste-cybercrime-risicos-van-thuiswerken-7-oplossingen

Welk advies zouden jullie geven: betalen van losgeld of niet doen?
Vanuit de overheid is het advies om geen losgeld te betalen aan criminelen, ook niet bij een cybercrime aanval. Door losgeld te betalen worden criminele activiteiten beloond en gestimuleerd.

FEITEN EN FABELS

1. **"Mijn bedrijf is niet interessant voor cybercriminelen…"**

Een veelvoorkomend misverstand! Jouw data is namelijk altijd interessant voor hackers. De reden dat jouw data waarde heeft voor criminelen is vaak niet omdat zij zelf iets met deze data kunnen, maar omdat deze data voor jou waarde heeft. Zonder deze data kun je je dagelijkse werk niet uitvoeren, waardoor het verliezen ervan veel schade oplevert. Een cybercrimineel weet dit en wil deze data daarom graag in handen krijgen en bijvoorbeeld met gijzelsoftware versleutelen. Als je bestanden eenmaal versleuteld zijn, is het vaak moeilijk om deze vrij te krijgen. De criminelen hebben je dan in een 'digitale houtgreep'.

2. **"Mijn wachtwoord is complex met speciale tekens en daarom nooit te raden…"**

Een veelvoorkomend misverstand! Een wachtwoord als bijvoorbeeld @uto! bevat vijf tekens en is gekraakt in drie minuten met een zogenaamde brute force aanval. Het is de lengte van het wachtwoord dat bepaalt hoe veilig het wachtwoord is, dus niet de complexiteit. Zie hieronder.

3. **"Tweestapsverificatie is niet nodig, want ik heb een lang wachtwoord…"**

Je hebt een lang wachtwoord en dan ben je er… toch? Niet helemaal. Gebruik naast een lang wachtwoord ook altijd een 'tweede stap' als verificatie. Mocht je je wachtwoord toch prijsgeven, kunnen hackers nog niet direct je account in. Door het instellen van tweestapsverificatie voeg je een extra beveiligingslaag toe aan je whatsapp, e-mailaccount of internetaccount waar je gebruik van maakt. Bij de belangrijkste accounts en diensten kun je dit zelf toevoegen.

4. **"Updates voer ik enkel uit als er interessante wijzigingen van toepassingen zijn…"**

Producenten van besturingssystemen, browsers en andere programma's, zoals Microsoft Office, Adobe Reader en Oracle Java, brengen geregeld updates uit om beveiligingslekken te verhelpen. Verouderde software is de belangrijkste oorzaak van hacks! Controleer in andere gevallen minimaal maandelijks of updates beschikbaar zijn en installeer deze dan zo snel mogelijk. Maak waar mogelijk gebruik van automatische updates.

5. **"Een openbaar wifi-netwerk kan ik gerust gebruiken om mijn zakelijke mail bij te werken…"**

Bij openbare en onbeveiligde wifi netwerken (free wifi) is het voor anderen mogelijk om te zien wat je op het internet doet en welke gegevens je verstuurt. Verstuur dus geen gevoelige gegevens (e-mail, internetbankieren) over netwerken die je niet kent of niet vertrouwt. Of gebruik een VPN. Versleutel thuis je draadloze netwerk met een lang wachtwoord om te voorkomen dat kwaadwillenden je internetverkeer kunnen onderscheppen.

6. **"Ik gebruik de cloud en loop daarmee geen risico om cyberslachtoffer te worden…"**

De cloud is als het ware een externe harde schijf, gekoppeld aan het internet. Deze cloud is vanuit iedere locatie te raadplegen, wat het een zeer gebruiksvriendelijke manier maakt om gegevens op te slaan. Zonder een uniek en lang wachtwoord met een tweestapsverificatie, is echter ook jouw cloud omgeving gemakkelijk te hacken. Dus ook hier blijft het belangrijk dat je aandacht hebt voor beveiliging.

7. **"Voor een cyber aanval moet je veel technische kennis hebben…"**

De wereld van de cybercrime professionaliseert in hoog tempo. Er zijn tegenwoordig zelfs websites waar criminelen simpelweg de software kunnen bestellen die ze nodig hebben voor hun digitale delicten: cybercrime-as-a-service (CAAS). Ook het niveau van dienstverlening stijgt: er zijn ransomware-bendes die over een helpdesk beschikken voor bedrijven die hebben betaald maar hun computersysteem niet opnieuw aan de praat krijgen. Door CAAS wordt het tegenwoordig helaas dus steeds makkelijker om cybercrime te plegen. Daarmee groeit ook het risico om slachtoffer te worden.

8. "Investeren in digitale veiligheid is voor mijn bedrijf te duur en weegt niet op tegen de baten…"

De jaarlijkse schade door cybercrime voor de Nederlandse economie bedraagt inmiddels meer dan 10 miljard(!) euro per jaar. In 2019 is ruim 55% van het midden- en klein bedrijf minstens één keer slachtoffer geworden van cybercrime. De schade door een digitale aanval loopt snel op, omdat je dagelijkse werkzaamheden niet meer (volledig) uitgevoerd kunnen worden. Hoewel investeren in preventie inderdaad geld kan kosten, is de schade die voorkomen wordt tientallen malen groter. De kosten wegen daarom ruimschoots op tegen de baten en dat maakt preventieve maatregelen juist relatief goedkoop. Tenslotte hoeven de basis cybersecuritymaatregelen niet duur te zijn.

9. "Ik doe geen aangifte van cybercrime, want dat is zinloos…"

Sommige mensen denken dat aangifte doen van cybercrime geen zin heeft, omdat de politie er niets mee doet. Dit is een misverstand. Iedere aangifte is namelijk een puzzelstukje om een zaak op te kunnen lossen. De realiteit is echter wel dat cybercriminelen wereldwijd en anoniem opereren. Het is daarom een grote uitdaging voor politie om deze criminelen te pakken en het oplossingspercentage is helaas laag. Toch blijft het heel belangrijk om te melden.

10. Mijn IT'er is verantwoordelijk voor mijn digitale veiligheid…"

Het is een veelvoorkomend misverstand: ondernemers die denken dat hun IT'er de digitale veiligheid regelt. Dit is niet vanzelfsprekend! Uw IT'er is voornamelijk bezig met het draaiende houden van uw systemen. Maar dit betekent niet dat hij per definitie aandacht (of kennis) heeft voor uw digitale veiligheid. Dit misverstand kan er voor zorgen dat u onbewust een groot risico loopt op schade door een digitale aanval. Of u nu een IT'er in dienst heeft of de IT heeft uitbesteed, het is in beide gevallen belangrijk om de situatie in beeld te hebben. Ons advies is dan ook om hierover in gesprek te gaan met uw IT'er en gezamenlijk uw digitale veiligheid te bespreken.