Nieuwsbrief 08

In deze **Nieuwsbrief**

- Security: Het wordt steeds gekker?
- Tien vuistregels voor Cybersecurity
- Phishing mails: Hoe herken je ze?
- Tips ter verlaging van risico's

Security: Het wordt steeds gekker?

Er bestaat tegenwoordig een App (KeyMe) waarmee je met je telefoon een foto kunt maken van je huissleutel en die kun je dan opslaan in een elektronische safe in "de cloud". Vervolgens ga je naar een kiosk van KeyMe en dan kun je met de informatie op de telefoon een duplicaat van die sleutel laten maken. In een artikel in Wired Magazine staat beschreven hoe je hier als hacker misbruik van kunt maken. Ten eerste kun je je afvragen of die informatie over jouw huissleutels wel veilig wordt opgeslagen in "de cloud". Aan de andere kant betekent dit dat je tegenwoordig dus ook je sleutelbos altijd in je zak moet houden om te voorkomen dat er stiekem een foto van je huissleutel gemaakt wordt.

Dit voorbeeld illustreert een groot probleem: Onbewust zijn van mogelijke gevaren en dreigingen. Wie verwacht er nou dat een sleutel middels een simpele App op een telefoon gedupliceerd kan worden? Bewustzijn bij medewerkers van elke organisatie op het gebied van de mogelijke gevaren en dreigingen is erg belangrijk. Eén van de hoofdconclusies van een KPMG security rapport uit 2013 was dat hackers een heel andere waarde hechten aan bepaalde zaken binnen een organisatie dan u of uw medewerkers. Dat gaat met name natuurlijk over de informatie die u in uw organisatie beschikbaar heeft. Als mensen bewust zijn van de gevaren begrijpen ze beter wat de consequenties kunnen zijn van onveilig gedrag. Technische oplossingen in het netwerk aanbrengen (firewalls, access management, intrusion detection, etc.) is niet meer afdoende. Ze helpen niets als de medewerkers van een organisatie onveilig gedrag vertonen.

Het veranderen van gedrag en het vergroten van het bewustzijn vergt goede training. Sebyde BV levert vanuit de Sebyde Academy goede Security awareness trainingen, workshops en thema sessies die erop gericht zijn om mensen te stimuleren en motiveren tot veilig gedrag.

Vraag **hier** meer informatie over de activiteiten van de Sebyde Academy

Tien vuistregels voor Cybersecurity

Het verlagen van de risico's op cybercriminaliteit begint bij het vergroten van het bewustzijn bij management en medewerkers. Cyber security zal daarvoor op de agenda moeten staan bij de bestuurders van een onderneming. Brancheorganisatie Nederland ICT heeft een aantal vuistregels geformuleerd waarover het management van elke organisatie moet hebben nagedacht.

1. Ik weet op welke manier ICT en Internet bijdragen aan de (vitale) bedrijfs- en productieprocessen van de organisatie en welke gegevens de organisatie beheert.
2. Ik weet welke risico's de organisatie loopt in geval van verstoring of cyberaanval, ook als deze verstoring elders in de keten plaatsvindt.
3. Ik weet aan welke eisen en regels de organisatie moet voldoen met betrekking tot gegevensbescherming
4. Ik weet wie in de organisatie verantwoordelijk is voor de beveiliging. Deze functionaris is voorbereid en heeft mandaat en voldoende middelen (bijv. 10% van ICT budget)
5. Ik zorg dat de organisatie richtlijnen heeft voor de beveiliging, o.a. over mobiel werken, de toegang tot systemen en het gebruik en het beveiligen van USB sticks en andere opslagmedia.
6. Ik zorg dat ICT systemen en netwerken van de organisatie goed beveiligd en up-to-date zijn en blijven.
7. Ik zorg dat het netwerk in de organisatie continue gemonitord wordt. Verdachte situaties worden snel opgemerkt en er wordt snel gereageerd op incidenten.
8. We laten de beveiliging regelmatig testen en oefenen de procedures periodiek.
9. De organisatie zorgt voor medewerkers die bewust zijn van cyberrisico's en hier in hun werk rekening mee houden. Ik geef als bestuurder zelf het goede voorbeeld.
10. Ik zorg dat de organisatie een plan heeft wat te doen bij een cyber incident, ook met betrekking tot de communicatie naar buiten de organisatie. Ik weet wie verantwoordelijk is en wie de besluiten mag nemen.

Phishing mails: Hoe herken je ze?

Iedereen heeft ze wel eens ontvangen: Phishing mails. Dit zijn emails die door hackers zijn rondgestuurd en waarbij ze proberen om je te verleiden om op een bepaalde (geïnfecteerde) link te klikken of om bepaalde (persoonlijke) informatie in te vullen. De mails lijken van een officiële instantie te komen, bijvoorbeeld een bank, de politie, of een creditcard bedrijf. Schijn bedriegt!

Ken je de afzender? Check altijd of email adressen en links wel refereren naar het "echte" bedrijf. Als het een vreemd adres is trap er dan niet in.
Is het iets onverwachts? Als je een email ontvangt van een pakketdienst dat een pakketje niet afgeleverd kan worden, vraag je dan af of je dat pakket wel verwachtte? Heb je recentelijk echt wel iets besteld bij een mailorder bedrijf? Als je een email ontvangt over je rekening bij bank XYZ en je hebt daar helemaal geen rekening kun je de mail ook direct deleten.

Zitten er spelfouten in de email? Veel phishing mails zitten boordevol grammaticale fouten. Verwijder dergelijke emails direct.
Is er een bestand als attachment toegevoegd? Kijk uit met het openen van bestanden. Met name in emails die je niet verwacht. Laat je niet verleiden door uitnodigende teksten als "AMAZING VIDEO" of "SPECTACULAR PICTURES".
Vraagt de email om persoonlijke informatie? Ga er maar rustig van uit dat er iets niet in de haak is als u om persoonlijke informatie wordt gevraagd. Zeker als het gaat om passwords, rekeningnummers, pincodes, etc. Trap er niet in. Banken zullen hun klanten nooit per email benaderen om dergelijke informatie te vragen!
Zit er een link in de email? Als je met de cursor over een link gaat (NIET klikken !!) verschijnt er een kleine window met de link waarnaar echt gelinkt wordt. Controleer of dit klopt.

Er bestaan leuke testjes om te kijken hoe goed u bent in het herkennen van Phishing mails. Vraag **hier** de link aan naar zo'n zelftest. Leuk om te doen en erg leerzaam!

Tips ter verlaging van risico's

Laat spreekkamers schoon achter!
Binnen spreekkamers wordt vaak gebruik gemaakt van whiteboards en/of flipovers. Na een bespreking wordt echter maar al te vaak vergeten om de informatie op deze whiteboards en flipovers te verwijderen of mee te nemen. Let maar eens op als u dergelijke kamers binnen komt. Deze informatie zou wel eens "interessant" kunnen zijn voor een klantrelatie die op een later tijdstip een bespreking heeft in die spreekkamer.

Biedt u WIFI aan? Sluit het na werktijd dan af.
Als u gratis WIFI aanbiedt, doe dat dan altijd met een passwordbeveiliging en verander dat password zéér regelmatig. Schakel indien mogelijk de WIFI na werktijd en in de weekenden uit. U wilt toch ook niet dat uw draadloze Internet toegang (WIFI) misbruikt wordt door hackers om ongeoorloofde activiteiten uit te voeren?

Kunnen wij u helpen?

Bij de security van web applicaties (websites), netwerken en systemen.

Het trainen van medewerkers of ontwikkelaars op het gebied van security awareness door de Sebyde Academy

Het doen van een management workshop ter voorbereiding van het implementeren van een Security Awareness programma.

Het laten controleren van de mogelijke privacy impact van uw informatiesystemen en organisatie.

U kunt contact opnemen via de volgende manieren:

Telefoon +31 6 53 23 32 69
Email rob.koch@sebyde.nl
Website http://www.sebyde.nl
Website http://www.sebydeacademy.nl

LinkedIn http://www.linkedin.com/company/sebyde-bv
Twitter http://www.twitter.com/SebydeBV
Facebook http://www.facebook.com/sebydeBV