Security als onderdeel van de bedrijfscultuur

Spreker: Carlo Klerk

cklerk@xebia.com

Carlo Klerk is security coach/ security specialist en helpt bedrijven om zelfstandig te worden op ICT security gebied. Voordat hij in 2007 security specialist werd was Carlo een hacker ("script kiddy") en pentester. Een pentester is een persoon die met toestemming gericht probeert de ICT systemen van een bedrijf of organisatie binnen te komen. Hiermee worden de zwakke plekken in de ICT security zichtbaar en kunnen daarna worden gedicht.

ICT security is een zaak voor iedereen. De menselijke factor is het grootste interne risico op cyber crime inbreuken voor bedrijven en organisaties. Carlo noemt de medewerkers daarbij niet de zwakste schakel binnen ICT security. Wel moeten medewerkers geholpen worden om een hogere bewustwording op cyber crime risico's te ontwikkelen. Als daarbij een "blame culture" ontstaat doordat bij security fouten schuldigen worden aangewezen en bestraft krijg je geen juiste ICT veiligheidscultuur. In een dergelijke angst cultuur zijn medewerkers bang om fouten te maken, tonen zij geen leef en leren niet van hun gemaakte tekortkomingen. Dit in tegenstelling tot het luchtvaart domein. De luchtvaart kent een "safety culture" en geen "blame culture". Incidenten en ernstige gebeurtenissen worden vanuit een "feedback loop" benaderd. Deze benadering zorgt ervoor dat risico oorzaken kunnen worden weggenomen. Zo heeft een Defensieblad "Vliegende Hollander" een rubriek gehad waarbij juist handelen werd behandeld waarmee mogelijke incidenten en of ernstige gebeurtenissen zijn voorkomen. Carlo noemt dit "in your face zetten". Je bespreekt met elkaar met voorbeelden uit de praktijk en vooral welke lessen hieruit geleerd kunnen worden.

Nederland is als land extreem "connected" met een grote dichtheid aan verbinden en snelle datalijn verbindingen. Er bestaat volgens Carlo Klerk niet zoiets als bewaking aan de landsgrenzen van ons internet, wij hebben dan ook weinig bescherming op inbreuken (cybercrime). Je moet zelf je eigen cyber verdediging organiseren. Bij veel bedrijven en organisaties leeft de gedachte bij de medewerkers dat de interne ICT security collegae de zaken zullen regelen: "wij hebben ICT security specialisten in dienst … dus dan zit het wel goed". Deze specialisten kunnen onmogelijk alle beveiligingssrisico's uitsluiten. Zij zoeken vooral naar wie een bedrijf of organisatie zou kunnen bedreigen. Daarna gaan zij gericht aan de slag in het netwerk ontwerp om het deze potentiële aanvaller(s) onmogelijk te maken om de ICT systemen aan te vallen of hier inbreuk op te maken. Wij noemen dit "security by design".

ICT security een zaak van ons allemaal omdat er een groot tekort aan ICT security specialisten is. Het is daarom beter om niet security medewerkers – ICT secure te maken. Je maakt medewerkers ICT secure door elkaar aan te spreken op gedrag, en voorbeelden uit de praktijk duidelijk te benoemen. Zorg dat fouten mogen worden gemaakt en geaccepteerd. Creëer een lerende omgeving waarbinnen de fouten worden gebruikt om met elkaar betere werkprocessen en systemen te krijgen. van en verbeter je jouw houding mee.

gebruik de verbindende factor – dreiging (kans x impact). Weet dat een verzekeraar bijvoorbeeld gemiddeld 3000 x per dag wordt aangevallen op haar ICT systemen, variërend van "aankloppen" tot zeer specifieke aanvullen op de DNS (domain name server) van een organisatie of bedrijf.

Na een uitgebreide kennismaking in een bedrijf of organisatie zoekt Carlo Klerk eerst zijn security champions. Deze haalt hij bij elkaar als "security chapter", die het kernteam met ICT skills vormen. Carlo geeft daarbij de tip om te zorgen voor een juiste mix in het kernteam. Er zijn mensen nodig die

iets kunnen, personen die zaken laten gebeuren met lef, en mensen die zorgen dat afspraken en plannen op tijd en volgens de juiste kwaliteit worden neergezet. Vervolgens worden de neuzen van het “security chapter” in dezelfde richting gezet. Aan iedere rol binnen de groep voegt Carlo kennis toe. Daarna kan deze groep mensen in het bedrijf of de organisatie met de “ICT security” bril aan het werk. Een gedegen communicatieplan met mensen uit het kernteam die kunnen binden en boeien, waarbij op enthousiaste wijze de successen worden benoemd en gevierd zorgt ervoor dat in de dagelijkse werkprocessen ICT awareness op een hoger plan komt en blijft.

Dan is het moment gekomen dat je als specialist weg kan omdat het bedrijf of organisatie zelfstandig verder kan met haar ICT security. Carlo Klerk is daarna als ICT security coach nog wel bereikbaar bij vraagstukken om te sparren. De oplossing voor het vraagstuk moeten zij zelf vinden.

Tot slot geeft Carlo nog enkele nuttige tips:

1. e-learning programma als Cybercrime is basic awareness en helpt niet voor blijvende ICT security in een bedrijf of organisatie.
2. blijven herhalen en vernieuwen (iedere dag worden niet cyber aanval methodes en werkwijzen ontwikkeld en door cybercriminelen toegepast)
3. gebruik vooral veel pakkende voorbeelden hoe en waar het fout is gegaan.

Tom van Staveren

Student MRM 8 - UTwente