‘40% van alle security incidenten wordt veroorzaakt door menselijk gedrag’

“Is het nu echt zo erg gesteld met informatiebeveiliging? Ik heb mijn systemen toch goed beveiligd?” Rob Koch van Sebyde vat samen hoe de meeste bedrijven denken over informatiebeveiliging. Een grote misvatting, stelt hij. “Bedrijven zijn steeds meer afhankelijk van ICT-systemen. Zonder deze systemen liggen de meeste bedrijven in grote mate stil. Ondernemers investeren daarom in goede systemen en in veiligheid. Maar hoe weet je nou zeker wanneer het goed genoeg is? Of is het wachten op de eerste keer dat het fout gaat? Bedrijven vragen zich af of het risico voor hun bedrijf wel zo groot is. Maar in feite is het niet de vraag OF een bedrijf slachtoffer wordt van cybercriminaliteit, maar wanneer.

Over welke risico’s hebben we het dan precies?
“Cybercriminelen zijn erop uit waardevolle bedrijfsinformatie te verkrijgen, te verminken of de bedrijfsprocessen te verstoren. De schade die zij aanrichten is groot. De schade aan ICT-systemen dient gerepareerd te worden, maar denk ook aan indirecte schade, zoals de bedrijfsreputatie die wordt aangetast.

Heeft u een voorbeeld van dit soort indirecte schade?
“De mogelijke gevolgen zijn zeer divers. Wat denken uw klanten van u wanneer door malware uw website automatisch wordt doorgesluisd naar een geïnfecteerde (porno)website? Ze verliezen door dergelijke incidenten het vertrouwen in uw bedrijf en lopen weg. Wat zijn de gevolgen als de salarissen niet op tijd verwerkt worden? Weinig bedrijven zijn goed voorbereid op een situatie waarin iets dergelijks zich voordoet.”

Doen bedrijven dan helemaal niks aan informatiebeveiliging?
“De meeste bedrijven nemen maatregelen aan de technische kant. Dit is de kant waarmee de ICT-ers binnen een bedrijf vertrouwd zijn en dus ook hun directie over kunnen adviseren. Dus denk aan een firewall, Access management, IPS, IDS, etc. Deze maatregelen zijn uiteraard ook nodig. Maar in veel gevallen niet de belangrijkste reden waarom het fout gaat. Menselijk handelen blijkt in 40% van de gevallen de oorzaak te zijn van security incidenten.”

‘Het is niet de vraag OF een bedrijf slachtoffer wordt van cybercriminaliteit, maar wanneer.’

Wat bedoelt u precies met menselijk handelen?
“Zelfs met de beste technische security oplossingen om uw netwerk tegen aanvallen van buitenaf te beschermen, zijn bedrijven nog steeds kwetsbaar. Als medewerkers bijvoorbeeld niet op de hoogte zijn hoe ze een phishing-mail kunnen herkennen is de kans groot dat ze een keer per ongeluk op een link in zo’n mail klikken. Of wanneer medewerkers onveilige of steeds dezelfde passwords gebruiken, maken ze het voor hackers wel heel makkelijk. Een ander voorbeeld van (onbewust) onveilig gedrag is het openlijk bespreken van vertrouwelijke (klanten)informatie in openbare ruimtes. Social engineers maken gretig gebruik van deze informatie die ze zomaar in de schoot wordt geworpen.”

Wat is dan de eerste stap naar veilig werken?
“Bewustwording. Het gaat erom dat iedereen binnen een organisatie beseft welke waarde de informatie heeft waarmee hij of zij werkt. En dat ze weten hoe ze er op een veilige manier mee om kunnen gaan. Iedereen in de organisatie draagt een stuk verantwoordelijkheid voor het beschermen van de informatie binnen een bedrijf.”

Makkelijker gezegd, dan gedaan, lijkt me. Hoe doet u dit?
“Het begint ermee dat bedrijven hun bezittingen inventariseren. En dan niet alleen het aantal servers, werkstations en printers in de organisatie. Maar juist ook informatie die is opgeslagen of verstuurd en ontvangen wordt. Wat is deze informatie je waard? Wie heeft er toegang tot die informatie? Is die informatie privacy-gevoelig? Zijn er betrouwbare backups? Het gaat vaak over veel meer informatie dan bedrijven vooraf beseffen. Dus niet alleen usernames en passwords, maar ook sales-/marketingplannen, prijsinformatie, bouwtekeningen, productlanceringen, patenten, klanteninformatie, email, agenda’s personeelsbestanden, correspondentie, financiële informatie, etc. Pas als je deze informatie, ook wel “de kroonjuwelen” genoemd, in kaart hebt weet je ook wat je moet beschermen.”

Kunt u enkele voorbeelden noemen van onveilig gedrag?
“Een veel gehoord voorbeeld is het gratis aanbieden van WIFI aan bezoekers. Er hangen bordjes met de inlognaam en het wachtwoord bij de receptie of in de spreekkamer. Wanneer kwaadwillenden dit lezen, kunnen ze ‘s avonds of in het weekend buiten op het parkeerterrein gaan staan en misbruik maken van uw internettoegang. Als hun criminele acties worden getraceerd, staat de politie uiteindelijk bij u op de stoep!”

Rob Koch (Sebyde)

Tip: schakel uw WIFI buiten werktijden uit en verander het password regelmatig.

“Een ander veelvoorkomend voorbeeld is wanneer mensen op reis zijn en een onbekend WIFI gebruiken, bijvoorbeeld in een restaurant, op een vliegveld of in een hotel. Een hacker kan heel eenvoudig zelf een WIFI netwerk opzetten en uw vertrouwelijke transacties onderscheppen.”

Ga veilig om met uw data! Stuur een mail naar membersbenefits@meeus.com en maak kans op één van de vijf beveiligde (8 Gb) USB-sticks!

Tip: wacht met het versturen van gevoelige informatie tot u zeker bent dat u op een (beveiligde) internet aansluiting werkt.

“Verreweg het bekendste voorbeeld van onveilig werken is de omgang met passwords. Je kunt het zo gek niet bedenken of je komt het nog tegen. Passwords op post-its op de monitor. Mensen die voor alle systemen hetzelfde password gebruiken. Mensen die passwords gebruiken die heel makkelijk te raden zijn. Denk aan opvolgende cijfers (12345), namen van kinderen of partner, geboortedata. Dit maakt het voor hackers wel heel makkelijk om in te breken in uw netwerk.”

Tip: weten hoe u veilig met wachtwoorden omgaat? Vraag het document ‘Tips voor veilig gebruik van Passwords’ aan via www.sebyde.nl

Wat kunt u doen?
Voer een degelijke risicoanalyse uit. Dan weet u welk risico u loopt en welke maatregelen het meest effectief zijn om uw veiligheid te waarborgen. Denk daarbij aan technische maatregelen, aan het bewustzijn van uw medewerkers, het inrichten van een veilige software-ontwikkelstraat en het verzekeren van de gevolgen van een security-incident.

Tip: informatie over het verzekeren van de gevolgen van cybercrime vindt u op meeus.com/cybercrime

Informatiebeveiliging is een continu proces. Verhoog het bewustzijn van uw collega’s over het risico en stimuleer veilig gedrag. Sebyde heeft hiervoor het Internet Weerbaarheid programma ontwikkeld voor management en medewerkers. Met dit programma brengen we duurzaam veilig gedrag in de organisatie.

Maak kans op een gratis workshop ‘Phishing’

Wilt u meer weten over hoe u uw bedrijf goed weerbaar maakt tegen cyberrisico’s? Vraag dan via info@sebyde.nl ons leaflet over de activiteiten van de Sebyde Academy aan. Dan maakt u bovendien kans op een gratis workshop ‘Hoe herken ik Phishing emails?’ voor twee personen.

Voor info: ga naar de website van uw brancheverenging, via Members’ Benefits (ledenvoordeel), tab Automatisering.