Een security-audit: geen overbodige luxe

In 2016 waren er per dag gemiddeld 53 inbraken in bedrijven, openbare instellingen en overheidsinstellingen. In de retail gebeurt 29% van de diefstallen door eigen personeel. Het zijn maar enkele cijfers die zaakvoerders of Facility Managers terecht aan het denken zetten. Beveiliging is meer dan ooit een hot item, maar in hoeverre is uw bedrijf gewapend tegen ongewenste bezoekers of interne diefstal? Een security-audit kan verhelderend werken. Kirsten Van der Hasselt van Trigion, een dochteronderneming van Facilicom, licht het hoe en waarom toe.

De tijden zijn voorbij dat vrij eenvoudige oplossingen, zoals een slagboom aan de toegangsweg, een stevige bewakingsagent of zelfs prikkeldraad als afschrikmiddel, volstonden om ongewenste bezoekers te ontmoedigen. Vandaag is het waarborgen van de beveiliging een stuk complexer geworden.

"Met een drone kijk je over muren heen", vertelt Kirsten Van der Hasselt, bij Trigion verantwoordelijk voor veiligheidsadvies. "Goedgevonden verhaaltjes volstaan soms om het vertrouwen van bewakers te verdienen en zo zelfs zonder badgelezer een draaitrommel te passeren. Met andere woorden: mensen met criminele intenties zijn creatiever dan we denken. Soms volstaat een klein testje al om zelf te kijken hoe goed je bedrijf beveiligd is en hoe makkelijk of moeilijk het bijvoorbeeld is om het archief of de serverruimte binnen te raken."

Blinde vlekken

Vaak schuilt het gevaar in kleine hoekjes. "Zo is er bij medewerkers soms onvoldoende bewustzijn rond veiligheid: ze laten waardevolle voorwerpen of documenten achteloos achter op bureau, stellen zich geen vragen als onbekenden op de afdeling rondlopen of laten bezoekers binnen, weliswaar met de beste bedoelingen. Er zijn nog andere risicofactoren, zoals: niet of onvoldoende beveiligde nooduitgangen of -trappen, beveiligde deuren die blijven openstaan of de omgeving. Wie zich namelijk bevindt in de nabijheid van gevangenissen, stations, ambassades of aardgasinstallaties, kan geteisterd worden door nevenschade als in de omgeving bijvoorbeeld aanslagen of andere calamiteiten gebeuren."

Last but not least is er nog 'het paard van Troje', zijnde: criminele intenties van eigen medewerkers. "Het is nuttig om te onderzoeken of iedere medewerker zomaar vrije toegang tot het hele bedrijf moet krijgen", vindt Kirsten Van der Hasselt.

Drie belangrijke stappen

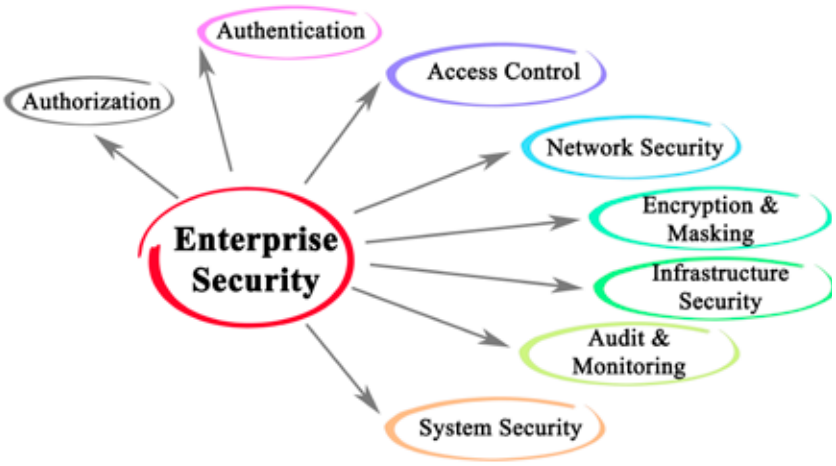
Wie dergelijke stille gevaren in kaart wil brengen, doet er goed aan een security-audit te laten uitvoeren bij een gespecialiseerd bedrijf. "In een eerste fase voe-

"Het is nuttig om te onderzoeken of iedere medewerker zomaar vrije toegang tot het hele bedrijf moet krijgen."
Kirsten Van der Hasselt, sales & security scans Trigion

ren we dan een kennismakingsgesprek waarbij we ook de grondplannen bestuderen, de incidenten van de voorbije jaren analyseren en interviews met belangrijke stakeholders voorzien. Zo komen we te weten welke voorschriften er gelden bij calamiteiten, welke procedures er zijn rond badgebeheer en toegangscontrole, hoe de opvolging van alarmen gebeurt, of er überhaupt wel camerabewaking of inbraakdetectie aanwezig is, et cetera. Vervolgens plannen we een volledige rondgang in en buiten het gebouw, waarbij we elke verdieping, ruimte en toegangsweg onder de loep nemen om een duidelijk 'helikopterbeeld' te krijgen. Op die manier ontdekken we de beveiligingsschillen, de kwetsbare punten en de plaatsen waar mensen eventueel kunnen indringen. Ook een omgevingsonderzoek en een analyse van regionale veiligheidsdata (waren er in de buurt recent brandstichtingen, diefstallen, gijzelingen,...) is nuttig."

"Een 'mystery visit' is een goede methode om het (klantvriendelijke?) gedrag van medewerkers te bekijken."

Alle bevindingen worden vervolgens gebundeld in een praktisch, oplossingsgericht en met veel foto's gestoffeerd security-rapport. "Het is de bedoeling dat je daar als bedrijf of instelling echt mee aan de slag kunt. Hierin omschrijven we de problematiek en brengen we een gedetailleerd risicoprofiel van het bedrijf, alsook de mogelijke gevaren waaraan de onderneming en haar medewerkers blootstaan, in kaart. Ook de efficiëntie van de huidige beveiligingsmaatregelen komt aan bod. Via een plaatsbeschrijving van gevoelige plekken en knelpunten krijgt de zaakvoerder of de Facility Manager een totaalbeeld van waar het bedrijf op vandaag staat qua beveiliging."
Een overzicht van 'quick wins' en maatregelen op langere termijn verduidelijkt wat er concreet moet gebeuren om de situatie te verbeteren. "Dat lijstje omvat fysieke en/of elektronische maatregelen, de creatie van procedures en voorschriften en/of trainingen om het veiligheidsbewustzijn bij het personeel te verhogen."



Bij medewerkers van een bedrijf is er vaak onvoldoende bewustzijn rond veiligheid. Soms volstaat een kleine zelftest al om te zien hoe goed je bedrijf is beveiligd. Regelmatig een security-audit laten uitvoeren, is een investering die zich snel terug verdient.

Mystery visits

Als het gaat om een gebouw dat regelmatig klanten, leveranciers of andere contacten over de vloer krijgt, kan een 'mystery visit' ook veel leren. "Hierbij proberen onze adviseurs incognito zo ver mogelijk in een onderneming te infiltreren. Het is ook een goede methode om het (klantvriendelijke?) gedrag van medewerkers te bekijken en te zien waar en hoeveel badges, handtassen en vertrouwelijke documenten worden achtergelaten. De bevindingen van een 'mystery visit' vormen vaak een goede basis om tijdens een vormingssessie het veiligheidsbewustzijn bij medewerkers te vergroten."

Relevantie

Regelmatig een security-audit laten uitvoeren, is een investering die zich sowieso terugverdient. "Zo'n onderzoek is vaak nuttig als er recent iets in de productie is veranderd, het bedrijf verhuisd is, de afdelingsstructuren veranderd zijn, er net een overname is gebeurd, noem maar op. Zowel grote als kleinere spelers zijn ermee gebaat, want iedereen wordt blootgesteld aan risico's. Het komt er eigenlijk op aan om criminelen, die hun werkwijze voortdurend bijschaven, altijd een stapje voor te zijn en geregeld na te gaan of de gebruikte beveiligingstechnieken nog niet achterhaald zijn."

Door Bart Vancauwenberghe

www.trigion.be

Vijf tips

1. Berg zoveel mogelijk op. Een rommelige omgeving nodigt uit tot stelen. Wie de principes van een clean desk nauwgezet toepast, heeft minder kans dat er iets verdwijnt.
2. Compartimenteer het gebouw. De installatie van een badgesysteem, met persoonsgebonden toegang tot ruimtes met een gevoelige inhoud, is een aanrader.
3. Organiseer, met respect voor het wettelijk kader, ad random uitgangscontroles.
4. Gebruik een registratiesysteem voor het uitlenen van materiaal.
5. Doe exitgesprekken met alle medewerkers die het bedrijf vaarwel zeggen, zeker als ze plots (moeten) opstappen.