HOE BELANGRIJK IS BEVEILIGING VOOR JE BEDRIJF?

'DE VRAAG IS NIET OF ER EEN INBRAAKPOGING KOMT, MAAR WANNEER'

Ieder bedrijf kan vandaag het slachtoffer worden van een poging tot inbraak. Wanneer de criminelen niet via een deur of raam proberen binnen te breken, vinden ze wel een manier om digitaal je onderneming binnen te glippen. Veel meer nog dan vroeger moeten bedrijven daarom preventieve maatregelen nemen om ongenode gasten buiten te houden. We verzamelden voor jullie zes beveiligingsexperts rond de tafel. Zij vertellen op welke wijze jouw bedrijf zich best beveiligt, zowel tegen fysieke als digitale bedreigingen.

Is beveiligen wel echt nodig? Hoe groot is de kans dat een bedrijf ongewenst bezoek krijgt?

Davy Ben Tahar - Securitas: Wanneer we spreken over fysieke inbraken is het niet zo eenvoudig om een percentage te noemen. De buurt waarin je bedrijf ligt, speelt een rol en ook de activiteit die je uitoefent heeft een grote invloed. Een magazijn vol met dure spullen zal sneller op de radar van inbrekers komen dan pakweg een afvalverwerkend bedrijf. Maar als dat laatste bij wijze van spreken de deur laat openstaan, zal daar dankbaar gebruik van worden gemaakt. Algemeen kunnen we zeggen dat criminelen de weg van de minste weerstand kiezen. Een inbreker herkent een slechte afsluiting of een kwetsbaar slot onmiddellijk. En heeft ook snel door wanneer een bedrijf camerabewaking of mobiele patrouilles inzet.

Pat Van Roey - VanRoey.be: Wanneer we over digitale inbraken spreken, is het veel eenvoudiger. De kans dat een cybercrimineel jouw onderneming probeert te infiltreren is 100%. De vraag is niet gaan ze proberen in te breken, maar wanneer. Of die poging slaagt, hangt af van de beveiliging.

Jo De Vylder - Proximus: Het digitaal inbreken is echt een industrie geworden. In 2016 is er in België ongeveer 330 miljoen euro geïnvesteerd in IT security. Anderzijds is er vorig jaar wereldwijd voor ongeveer 300 miljard euro schade toegebracht door cybercriminaliteit. Het spreekt dan ook voor zicht dat criminele organisaties zich meer en meer toeleggen op deze activiteiten (zoals IS bijvoorbeeld).

Emanuel van der Aalst - Netropolix: Probleem is dat bedrijven vaak niet eens weten dat ze getroffen worden door cybercriminelen. Door het Internet of Things (IoT) zijn meer en meer bedrijfsinfrastructuren verbonden met het internet. Een gebrekkige beveiliging speelt dan sterk in de kaart van mensen met kwade bedoelingen.

Pat Van Roey: Naar schatting is de helft van de bedrijven geïnfecteerd zonder dat ze het weten. En geïnfecteerd wil zeggen dat er data, kostbare informatie dus, verdwijnt.

Aangezien bedrijfsleiders goede huisvaders zijn, kunnen ze dus niet anders dan investeren in beveiliging?

Gust Dierckx - DNCS: Inbraakbeveiliging is vandaag in ieder geval een logische keuze. Enkele jaren geleden - toen we nog met analoge camera's moesten werken – ging het prijskaartje voor een degelijk beveiligingssysteem snel de hoogte in. Zeker voor wat kleinere KMO's was dat toch een barrière. Met de digitale systemen van vandaag is een goede beveiliging eigenlijk voor iedereen een haalbare kaart.

Gunter Roefs - GR-Technics: En niet alleen met camera's. Dankzij de verbeterde technieken kunnen we bedrijfsterreinen en gebouwen veel beter en gerichter verlichten. Een goede verlichting is nog steeds een uitstekende manier om vandalisme en diefstal tegen te gaan. En doordat we die verlichting en camera's kunnen koppelen aan allerlei sensoren, gaan ze enkel werken wanneer nodig.

Davy Ben Tahar: Sensoren die op hun beurt onze mensen gaan waarschuwen, waardoor die snel en efficiënt ter plaatste kunnen komen. Alleen denken we meestal dat zoiets bij ons wel niet zal gebeuren. We gaan daardoor vaak pas actie ondernemen en investeren in beveiliging wanneer er een incident heeft plaatsgevonden. En dan zijn er twee keer kosten.

Gunter Roefs: Wat heel jammer is. Bedrijven beseffen ook te weinig de impact van een soms kleine diefstal. Uiteraard kost enkele meters kabel vervangen die gestolen zijn op een werf niet zoveel. Alleen ga je zien dat dit type kabel net dan niet in voorraad is, waardoor je ploeg een dag of langer stilligt. En maak dan de rekening maar eens.

Jo De Vylder: De digitale beveiliging is nu ook voor de overheid een prioriteit geworden. Op 28 mei 2018 moet elk bedrijf die met persoonsgegevens werkt, voldoen aan de General Data Protection Regulation (GDPR). Is een bedrijf niet in orde met de wetgeving, kan dit grote gevolgen hebben. Eén klacht kan leiden tot een audit en boetes die oplopen tot 20 miljoen euro of 4% van de totale wereldwijde jaaromzet van het voorafgaande boekjaar.

Securitas takes cares of your security

At home

On the road

At work

Anywhere

Tel 02 263 24 42 · sales@securitas.be · www.securitas.be

Vergunning FOD BiZa nr. 16.1055.04

SECURITAS

Emanuel van der Aalst: Praktisch betekent dit dat bedrijven bij een incident moeten kunnen bewijzen dat ze al de mogelijke technische en organisatorische maatregelen genomen hebben om gevoelige data te beschermen.

Pat Van Roey: Maar ook hier zijn bedrijven zich te weinig bewust welke schade dataverlies tot gevolg kan hebben. Statistisch heeft een bedrijf dat zijn data verliest nog 40% kans om te overleven. Dat wil zeggen dat 60% de boeken mag dicht doen.

Ok, we zijn overtuigd. Welke stappen moeten we zetten voor een goede beveiliging?

Gust Dierckx: Om te beginnen met je ervoor zorgen dat er een zeer goed operationeel netwerk aanwezig is. Dat heb je nodig zowel voor je fysieke bewaking, als voor het beveiligen van je data. Er zijn sowieso heel wat raakvlakken tussen de twee manieren van beveiligen. Wanneer je een grote site hebt met soms twee tot driehonderd camera's, dan is er software nodig om die camera's vlot te monitoren.

Davy Ben Tahar: Het is ook belangrijk om te beseffen dat het bewaken al buiten je bedrijf start. Een camera hangen, waardoor je ziet dat er iemand binnengebroken is, volstaat niet. Dan kan je enkel op band bekijken wat ze meegenomen hebben. Je moet eigenlijk een perimeter rond je bedrijf voorzien, waardoor je in staat bent om voor de inbraak al te reageren via bijvoorbeeld een mobiele patrouille.

Emanuel van der Aalst: Bij beveiliging moet je ook altijd in het achterhoofd houden dat de mens de zwakke schakel is. Dat is zo bij het fysiek bewaken van je bedrijf. Iemand vergeet bijvoorbeeld om goed af te sluiten. Of een bewakingsagent is net de ruimte uit, wanneer iets op de monitor verschijnt. Dat moet je dus incalculeren. Maar dat is net zo bij het beschermen van je data. Medewerkers verliezen hun smartphone of laptop. Iemand werkt op verplaatsing, maar staat er niet bij stil dat de internetverbinding daar niet veilig is. Of je krijgt gewoon een mail en door het openen van de bijlage zet je de digitale deur wijd open.

Pat Van Roey: Een nuttige tip : De HR dienst is waarschijnlijk het meest kwetsbare deel van een organisatie. Elke bedrijf is op zoek naar mensen en publiceert vacatures met gerichte vragen. Het is niet moeilijk voor criminelen om een zeer geloofwaardige mail met bijlage of link te sturen die een medewerker van HR, zonder van enig kwaad bewust te zijn, zal openen waarna malware , zoals bvb cryptolocker , zich zal verspreiden over het netwerk. Een degelijke sandbox is dan ook geen overbodige luxe voor eender welke organisatie.

Gust Dierckx: Monitoren gaat hierdoor steeds belangrijker worden. Je moet zorgen voor een goede beveiliging, maar je moet ook weten wanneer die beveiliging op de proef gesteld wordt. Want uit elke poging tot inbraak kan je iets leren.

Jo De Vylder: Het beveiligen van de bedrijfsomgeving en diens data blijft een continu en snel evoluerende noodzaak. De cybercriminelen gaan steeds inventiever tewerk waardoor je beveiliging nooit 'af' is. De noodzaak voor gespecialiseerde en diep technische IT security kennis blijft groeien wat meer en meer bedrijven naar een managed service doet uitkijken.

Kan je nog op eigen houtje in je beveiliging voorzien?

Gunter Roefs: Ik denk het niet. Een kleine vandaal of een gelegenheidsdief ga je misschien nog kunnen afschrikken met een setje uit de doe-het-zelf-zaak. Maar de professionele bendes die actief zijn, schrik je hiermee niet af. Bedrijven mogen beveiliging ook niet zien als een kost, het is een investering. Daarom ook dat je recht hebt op fiscale aftrek, wanneer je de werkomgeving goed gaat beveiligen.

Gust Dierckx: Je moet ook de wetgeving heel goed kennen. Je mag niet zomaar iedereen filmen of data verzamelen. Een beveiligingspartner weet wat kan en mag.

Davy Ben Tahar: Dat klopt. Een partner kan een veiligheidsscan op maat van jouw bedrijf ontwerpen en integreert verschillende veiligheidsoplossingen tot een logisch geheel. Hoewel 100% beveiliging niet bestaat, zal dit ervoor zorgen dat je goed beveiligd bent en tegelijk overbodige kosten uitsparen.

Emanuel van der Aalst: Zonder professionele partner je data gaan beschermen is al helemaal een groot risico. Je software moet altijd up to date zijn, hackers gaan gebruik maken van de kleinste opening. En wanneer achteraf blijkt – zeker met de nieuwe GDPR-wetgeving – dat je zelf in de fout ging, kan dat zeer veel geld kosten.

Jo De Vylder: Door de toegenomen complexiteit, is de hulp van een gespecialiseerde partner noodzakelijk. Niet alleen de perimeter beveiliging, maar ook de intern datastromen en infrastructuur dient geanalyseerd te worden. Laat in ieder geval regelmatig een expert een assessment uitvoeren, zodat de zwakheden van je systeem in kaart gebracht worden en daarna weggewerkt. Security kan maar werken als er een 360° aanpak wordt toegepast bestaande uit Preventie, Detectie, Behandelen en voorspellen.

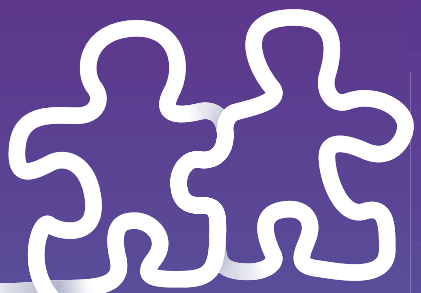
Pat Van Roey: Met de hulp van een goede partner, heb je een streepje voor op de hackers. Een antivirusprogramma of een firewall bieden geen afdoende bescherming meer. Je hebt een beveiligingsomgeving nodig die uit meerdere lagen bestaat. Bovendien is het beveiligen van de perimeter niet meer voldoende. De zwakste schakel blijft de (al dan niet bewuste) mens en het gevaar komt meestal van binnen je organisatie. Bijvoorbeeld een device wordt geïnfecteerd via een USB-stick en zal van binnenuit informatie naar buiten brengen zonder dat men iets merkt. Je medewerkers trainen in het veilig omgaan met bedrijfskritische informatie is essentieel.

Gust Dierckx: En dat is geen overbodige luxe. Bedrijven die op vijftig jaar zijn opgebouwd, kunnen vandaag in enkele dagen volledig van de kaart worden geveegd. Je kan dus beter voorkomen, dan genezen.

Wat is goede service voor u ?

"Iemand
die klaarstaat.
Vandaag."

"Iemand die mijn
bedrijf klaarmaakt.
Voor morgen."



Bij Proximus staat er altijd een contactpersoon voor u klaar, die u en uw bedrijf persoonlijk kent. Iemand die uw IT-en telecomvragen snel beantwoordt en ook actief meedenkt. Zo komen we samen tot de juiste oplossingen die uw bedrijf verder helpen groeien.

Ontdek onze persoonlijke service op

proximus.be/nieuwperspectief

proximus

Altijd dichtbij

AAN DE TAFEL

Pat Van Roey
General Manager VanRoey.be

VanRoey.be denkt met je mee over de hele ICT binnen jouw organisatie. Zo kan je je concentreren op jouw kernactiviteiten. In plaats van reactieve diensten bij storingen, legt het bedrijf de focus op proactieve ICT diensten om storingen te vermijden, zodat je geen tijd verliest. Cybersecurity bij klanten krijgt zeer veel aandacht binnen VanRoey.be. Het bedrijf zorgt dat jouw organisatie op alle niveaus voldoende beveiligd is tegen externe en interne bedreigingen. Hun Missie : 'We are the trusted guide on your digital journey so you can create wonderful things'.

Emanuel van der Aalst
Chief Evangelist Netropolix

Netropolix heeft als missie & slagzin: IT op de Achtergrond. Wij houden van IT, maar begrijpen dat de klant gewoon wilt dat het werkt. Binnen het bedrijf hebben we zowel een software huis als een hardware afdeling. Onze programmeurs staan u bij om bedrijfsprocessen te vertalen en te automatiseren waar onze technici ervoor zorgen dat uw bedrijf dag en nacht kan blijven draaien. Netropolix is stevig verankerd in de Kempen met vestigingen in Geel, Turnhout en Grobbendonk.

Jo De Vylder
Sales Manager Security Specialists Proximus

Proximus is aanbieder van geïntegreerde digitale diensten zowel op telecommunicatie als IT gebied. Vanuit Proximus Security zetten we in op de 360°graden aanpak, wat niet alleen focust op perimeter beveiliging maar ook op bescherming van de vertrouwelijke gegevens en computersystemen in een managed aanbod. Het Proximus aanbod biedt naast oplossingen ter bescherming tegen, ook expertise tijdens de cyber aanvallen als in de nasleep en voorspelling hiervan.

Davy Ben Tahar
Sales Consultant regio Antwerpen Securitas

Securitas is een bewakingsonderneming van Zweedse origine/oorsprong. In België zijn ze actief op verschillende vlakken, gaande van mobiele bewaking, meldkamerdiensten en statische bewakingsagenten zowel voor KMO's, grote bedrijven & overheid als voor particulieren. Securitas combineert mensen, technologie en kennis in sterke security solutions voor elke situatie.

Gust Dierckx
zaakvoerder DNCS

DNCS is een netwerk expert die integreerbare en schaalbare beveiligingsinstallaties aanbiedt die eenvoudig centraal en remote te beheren zijn. Zo wordt een zorgeloos facility beheer mogelijk oa door overzichtelijke procesopvolging en het opleveren van betrouwbare analyses. Het bedrijf werkt voor toekomstgerichte KMO-ondernemers en beveiligingsverantwoordelijken van bedrijven en overheden. DNCS heeft met deze klanten een zeer persoonlijke en projectgedreven langetermijnrelatie.

Gunter Roefs
zaakvoerder GR-Technics

GR-Technics uit Beerse is specialist en marktleider in het produceren van mobiele camera- en lichtmasten en alle werfverlichting in de Benelux en in verschillende Europese landen. Deze worden voornamelijk ingezet op bouwwerven, industriële toepassingen, festivals, evenementen en sportmanifestaties. Met een team van negen enthousiaste medewerkers staat het bedrijf iedere dag klaar om te streven naar de meest kwaliteitsvolle producten. GR-Technics is actief in zeven Europese landen en het bedrijf heeft dankzij zijn innovatieve oplossingen voor tijdelijke verlichting en veiligheid een portefeuille opgebouwd van meer dan 120 trouwe klanten.