GET
Azkoyen Time & Security Division

Tijd om uw bedrijf écht goed te beveiligen

Laat uw toeganscontrole niet in de kou staan

"We take care of you, while you take care of your business!"

Tijd om uw bedrijf écht goed te beveiligen

Laat uw toegangscontrole niet in de kou staan

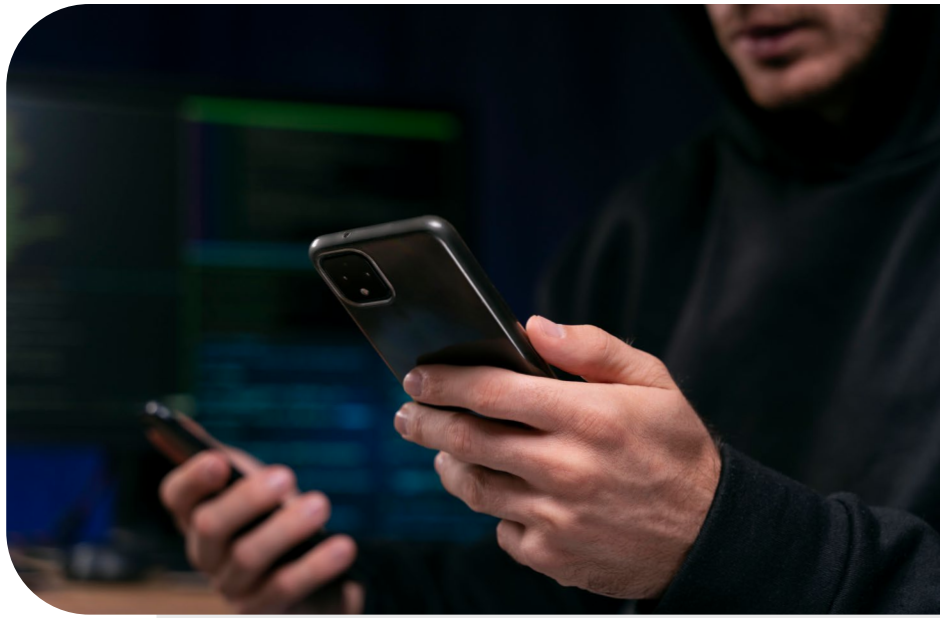
Cybersecurity, hét onderwerp waar techjournalisten, experts en vrijwel iedereen die op één of andere manier te maken heeft met ICT, maar niet uitgepraat over lijken te raken. Na wat onfortuinlijke incidenten, datalekken en andere spraakmakende voorvallen in de afgelopen decennia, is het veilig houden van de digitale infrastructuur een topprioriteit geworden bij vrijwel elk bedrijf. En omdat de wereld van cybersecurity nu eenmaal grillig is en van jaar tot jaar sterk verandert, aarzelen de meeste (grote) bedrijven niet om jaarlijks miljoenen euro's te steken in de crème de la crème op het gebied van digitale veiligheid. Het is een begrijpelijke denkwijze, die er maar al te vaak in resulteert dat de fysieke bedrijfsbeveiliging, zoals bijvoorbeeld toegangscontrole, achterblijft. Want, "Medewerkers hebben een eigen badge waarmee ze binnen komen. En dat gaat al jaren goed, op dezelfde manier. Waarom nu veranderen?". Dit is een veelgehoorde uitspraak als het onderwerp ter sprake komt. En daar zit, helaas, een gevaarlijke denkfout in. Een fout die kan leiden tot onherstelbare schade en veel onnodig leed… ■

Toegangsbadges kunnen óók gehackt worden

"Als het werkt, dan werkt het". Dat is de insteek waarmee veel bedrijven hun toegangscontrole benaderen. Medewerkers krijgen een eigen badge die de deuren opent, waardoor ongewenst bezoek in de kou blijft staan. En dat gaat in principe al tien, vijftien of zelfs twintig jaar goed. En dus lijkt er op het eerste gezicht geen enkele reden om dingen anders te doen. De wereld van cybersecurity mag dan misschien in rap tempo veranderen, maar de oude, vertrouwde badges en scanners doen gewoon hun werk. Niet?

We zien deze denkwijze veel terug. En dat heeft er waarschijnlijk mee te maken, dat veel bedrijven (en zelfs de ICT-experts aldaar) er wellicht niet van op de hoogte zijn dat toegangsbadges óók gehackt kunnen worden. Want, niet alleen cybersecurity verandert constant, ook criminelen maken steeds vaker gebruik van digitale middelen om zich toegang te verschaffen tot fysieke locaties. En dat kan tegenwoordig "gewoon" met de smartphone. Een voorbeeld: als cybercrimineel hoef je, met de juiste applicatie, alleen maar even je GSM tegen de broekzak van een nietsvermoedende medewerker te houden om álle data die zich op de verouderde toegangsbadge ín die broekzak bevindt, over te nemen. Daarna kan deze crimineel de toegangsbadge één op één namaken. En dat allemaal, zonder dat de onfortuinlijke medewerker wiens badge zojuist gekopieerd is, dit in de gaten heeft. Het lijkt onwaarschijnlijk, maar dit is slechts één van de risico's die je loopt als uw systeem voor toegangscontrole ouder dan vijftien jaar, of zelfs tien jaar is.

Niet alleen cybersecurity verandert constant, ook criminelen maken steeds vaker gebruik van digitale middelen om zich toegang te verschaffen tot fysieke locaties.



Miljoenen naar cybersecurity
en tóch een inbraak

Oude badges zijn dus met het grootste gemak te kopiëren. En dat heeft desastreuze gevolgen voor de veiligheid van uw bedrijf. Een oude badgelezer zal immers nooit herkennen dat een badge gekopieerd is. En dat zorgt er voor dat criminelen dus vrij letterlijk gewoon naar binnen kunnen wandelen via de achterdeur, of zelfs via de voordeur. En ook binnen in uw pand gaan alle deuren gewoon open, nét zoals ze zouden doen voor de medewerker wiens badge gekopieerd is. En als een crimineel eenmaal binnen is, kan het snel gaan. Hypothetisch gezien is een USB-stick met ransomware en cryptolockers nu álles wat er nodig is om uw hele bedrijf plat te leggen, of om waardevolle data of zelfs geld te stelen. Als de crimineel eenmaal binnen is en de deuren open zijn, hoeft deze persoon enkel en alleen maar een PC te vinden die is aangesloten op het lokale netwerk. De USB kan dan in de USB-port en de schade is aangericht. Tegen zo'n inbraak kan zelfs de beste cyberbeveiliging niets uitvoeren.

Valse beschuldigingen
en emotionele schade

De datalog van uw toegangssysteem kan waarschijnlijk traceren welke deuren op welk moment geopend zijn. En als de inbraak eenmaal ontdekt is, is het logisch dat er gekeken wordt naar de verantwoordelijke badge. En u zult zien: de sporen wijzen vervolgens allemaal naar uw nietsvermoedende medewerker, wiens badge gekopieerd is. Vervolgens komt hij of zij onterecht als verdachte in beeld en is naast de materiële schade, ook de emotionele schade ondenkbaar groot. Als de medewerker in kwestie bijvoorbeeld géén verifieerbaar alibi heeft, dan kan dit een lang en slepend onderzoek als gevolg hebben. Kortom, álles aan deze situatie wilt u als directeur, of hoofd van de ICT-afdeling, koste wat kost voorkomen. En dan wijzen alle pijlen toch richting het verbeteren van uw bedrijfsbeveiliging.

Nieuwe technologie is nagenoeg ondoordringbaar

Voor de veiligheid van uw bedrijf is het ondenkbaar dat u miljoenen euro's in cybersecurity steekt, om vervolgens geen oog te hebben voor het feit dat uw toegangscontrole zo lek is als een mandje. Dat kan en moet dus anders, voor u, uw gegevens en uw medewerkers. Daarom is het de hoogste tijd dat u uw badges, badgelezers en de onderliggende infrastructuur laat vervangen door nieuwere, veiligere technieken zoals bijvoorbeeld de MIFARE DESFire. Uw medewerkers kunnen gewoon, net als vanouds met een eigen badge of toegangspas de deuren openen. Alleen laten deze nieuwe technieken zich niet hacken op kopiëren, omdat ze versleuteld zijn met state of the art encrypties die net als uw oude software gewoon jarenlang meegaan. En daarnaast bieden nieuwe badges dankzij technologische innovatie ook nieuwe voordelen, zoals het uploaden van saldo voor waarmee betaald kan worden in de kantine. Zo wordt uw bedrijf niet alleen veiliger, maar ook vriendelijker voor uw medewerkers. ■

Voor de veiligheid van uw bedrijf is het ondenkbaar dat u miljoenen euro's in cybersecurity steekt, om vervolgens geen oog te hebben voor het feit dat uw toegangscontrole zo lek is als een mandje.

Het is tijd om uw bedrijf echt te beveiligen

Laten we voorop stellen dat het úiteraard van groot belang is dat uw cybersecurity op orde is. Maar, op het moment dat de toegangscontrole van uw bedrijf sterk verouderd is, kunnen de vele lagen aan cyberbeveiliging helaas niets uitvoeren. En dan loopt uw bedrijf nog altijd een onnodig risico op inbraken, met alle gevolgen van dien. Gelukkig zijn er nieuwere, veiligere technieken die uw bedrijf écht veilig houden, zonder dat er structureel iets verandert in de manier waarop uw medewerkers 's ochtends de deur openen. Maar één ding is zeker: criminelen blijven ditmaal écht in de kou staan. ■

Bent u er klaar voor om uw bedrijf écht te beveiligen? Dan gaan we graag met u in gesprek om de mogelijkheden te bespreken. Zo wordt uw onderneming straks ondoordringbaar op álle fronten!

Samen verder praten?
Dan kunt u ons bellen op +32 (0)3 312 92 30.
We spreken u graag!

GET
Azkoyen Time & Security Division

GET nv
Antwerpsesteenweg 107
2390 Malle, België
+32 3 312 92 30
info@get.be
www.get.be

GET Nederland bv
Albert Einsteinweg 4
8218 NH Lelystad, Nederland
+31 320 25 37 90
info@get.nl
www.get.nl