NRB

DARING TO COMMIT

UW GEGEVENS BESCHERMEN OM UW ONDERNEMING TE BESCHERMEN

CYBERSECURITY IS BELANGRIJK VOOR DE PRIVATE EN PUBLIEKE SECTOR, VOORAL OMDAT ER NOG NOOIT ZO VEEL AANVALLEN ZIJN GEWEEST.

"*Een veilige computer is een uitgeschakelde computer. En dan nog...*"

Dit citaat van Bill Gates dateert van het begin van het millennium. Twintig jaar geleden was cyberveiligheid al een hot item. Vandaag blijft dit probleem zich in een indrukwekkend tempo verspreiden, vooral na de laatste gebeurtenissen die de wereld de afgelopen jaren hebben geschokt. "*De lockdown door het coronavirus en de oorlog in Oekraïne hebben sterk bijgedragen aan een toename van online aanvallen* ", bevestigt Vincent Ceriani, hoofd Cyber Risk Services bij de NRB-groep.

Er zijn meer dan genoeg voorbeelden van gegevensdiefstal. Elke week duikt er een nieuwe zaak op en de gevolgen kunnen desastreus zijn. Grootsteden, ziekenhuizen en bedrijven zijn het doelwit van hackers die altijd op zoek zijn naar een slachtoffer om hun aanval op te richten. "*Kleinere bedrijven zijn bang om geld te verliezen of dat hun productie voor weken stilgelegd wordt. Grote bedrijven zijn bang dat hun reputatie wordt beschadigd* ", verklaart Lorenzo Bernardi, Head of Security Services van NRB.

De bedreigingen zijn bekend, net als de aard van de aanvallen. "***Hacken en ransomware zijn de twee trends***, *als ik het zo mag zeggen. Zo zijn in de eerste drie maanden van dit jaar al twee van onze klanten gehackt* ", zegt Lorenzo Bernardi. "*Kwaadwillenden kunnen bezitnemen van gegevens omdat updates niet regelmatig zijn uitgevoerd. Dat is een eenvoudige handeling, maar nog te veel bedrijven hebben deze reflex niet. Iedereen heeft het over cyberveiligheid, maar in werkelijkheid is er een echt gebrek aan kennis op dit gebied*."

De expertise van de NRB-groep wordt erkend in de private en publieke sector. Dit blijkt uit het feit dat het zakencijfer van de cyberbeveiligingsactiviteiten in de afgelopen vier jaar is verzesvoudigd en in de eerste drie maanden van 2023 de waarde van de contracten voor het jaar 2022 al is overschreden. "*Dat is niet verwonderlijk omdat er steeds meer verbonden systemen zijn. Alles is geautomatiseerd en criminele organisaties hebben begrepen welk financieel belang zij daaruit kunnen halen* ", beschrijft Vincent Ceriani.

HET PROBLEEM: GEBREK AAN KENNIS

Cybersecurity is een regelmatig terugkerend onderwerp in de media en in bedrijven. Het opzetten van **een goede verdedigingsstrategie is echter niet zo eenvoudig** omdat alles nieuw lijkt. "*Laten we het voorbeeld nemen van het telewerken dat tijdens COVID in opmars was. Er werden heel wat oplossingen voor telewerken gelanceerd zodat werknemers in de beste omstandigheden thuis konden werken. Helaas hebben sommige organisaties geen sterke authenticatie ingebouwd, en was er bijvoorbeeld geen tweede authenticatie via de mobiele telefoon. In dat geval heeft de hacker alleen een naam en een wachtwoord nodig om te kunnen inbreken. Zodra hij in het systeem van het bedrijf is gepenetreerd, staan alle gegevens tot zijn beschikking* ", vervolgt Vincent Ceriani.

Deze gegevens verkrijgen kan met één enkele klik. "*Stel: een medewerker van het secretariaat, dat zich onvoldoende bewust is van beveiliging, opent een e-mail waarin ze hem beloven dat hij een dure telefoon kan winnen als hij zijn naam, telefoonnummer en wachtwoord opgeeft. De hacker krijgt deze gegevens van hem en kan elke gewenste actie ondernemen. Een klant vertelde me onlangs dat een hacker de verzending van factuurmails had tegengehouden, ze had bewerkt met zijn rekeningnummer en ze vervolgens weer naar klanten had gestuurd. U kan zich inbeelden welke de gevolgen dit had...*"

Bedrijven zijn verantwoordelijk voor de persoonsgegevens waarover zij beschikken, of het nu gaat om hun personeel of hun klanten. Daarom is de Algemene Verordening Gegevensbescherming (AVG) in april 2016 gestemd, maar de inhoud ervan is nog te weinig bekend bij het grote publiek. "*Ik heb soms de indruk dat sommige mensen deze wet pas leren kennen. Als een hacker gegevens steelt, wordt het bedrijf verantwoordelijk gehouden. Onlangs legde een klant mij uit dat hij een blad papier met klantinformatie en een rijschema aan zijn bezorgers gaf. Dat is op zich geen probleem, tenzij zijn bezorgers het blad bij de laatste klant achterlaten omdat die het niet meer nodig hebben. In dit geval bezit de klant de gegevens van alle andere klanten (adres, telefoonnummer...)*", legt Vincent Ceriani uit.

— **Vincent Ceriani**
Head of Cyber Risk Services van de NRB–groep

Gelukkig zijn deze problemen niet onoplosbaar. "***Hackers zijn zeer goed getraind***, *maar er zijn normen en maatregelen om ze af te remmen* ", zegt Lorenzo Bernardi. "*Het CCB (Centrum voor Cybersecurity België) maakt bedrijven steeds meer bewust van deze problematiek. Het Waals Gewest voert ook initiatieven op verschillende niveaus (opleiding, onderwijs, samenleving) op, zoals de Cyber Security Coalition.*"

PENETRATIETESTS TIJDENS DE OORLOG IN OEKRAÏNE

Gegevensbeveiliging is een groot maatschappelijk probleem. Helaas kan niet iedereen zich een audit via een penetratietest veroorloven. De NRB-groep heeft zijn diensten aan vzw's en scholen aangeboden bij het begin van de oorlog in Oekraïne, een moment dat door hackers werd uitgekozen om hun aanvallen op te voeren. "*Het was belangrijk om onze competenties in dienst te stellen van het volk en het land. Daarom besloten we tijd en personeel vrij te maken om iedereen te helpen die dat het meest nodig had* ", aldus Lorenzo Bernardi.

DE NRB-GROEP, ERKEND SECURITY EXPERT

De NRB-groep investeert in cybersecurity en biedt zijn klanten een complete dienstverlening. **Onze experts kunnen zowel op wettelijk niveau en dat van de compliance, als op technologisch niveau optreden**. "*Deze combinatie is volgens ons een geslaagd beveiligingsplan. Door op al deze niveaus te werken, kunnen we deze strijd winnen* ", zegt Lorenzo Bernardi.

Om aan de behoeften van zijn klanten te voldoen, werft de groep voortdurend veiligheidsspecialisten aan. Ze krijgen een volwaardige opleiding. "*Een IT-specialist kan niet een heel bedrijf beveiligen, dat is een vak apart. Er is een tekort aan specialisten in België, in die mate dat er enkele duizenden vacatures zijn. NRB speelt hierbij een fundamentele rol door jonge medewerkers aan te werven en hen vervolgens op te leiden in alle aspecten van de beveiliging. We kunnen bijna zeggen dat we een talent factory zijn* ", besluit Lorenzo Bernardi.

Ons bedrijf beschikt over een **complete catalogus** om zijn klanten de beste service te bieden.

1. De groep is actief in het voorkomen van aanvallen van binnen en buiten de onderneming. De resultaten zijn al opmerkelijk, met verbeterde bescherming tegen ransomware en sensibiliseringscampagnes in de hele onderneming.

2. Onze experts zijn ook gespecialiseerd op het gebied van opsporing. Zij voeren beveiligingsaudits uit bij onze klanten, onder andere via 'ethisch hacken'. Op basis van de vaststellingen stellen zij een roadmap voor beveiligingsverbeteringen op.

3. Wij helpen bedrijven die het slachtoffer zijn geworden van een cyberaanval bij het herstellen van hun gegevens en bieden hen ondersteuning op het gebied van regelgeving (AVG).

4. Onze groep is ISO 27001 gecertificeerd. Onze experts ondersteunen onze klanten bij hun eigen ISO 27001-certificering.

— **Lorenzo Bernardi**
Head of Security Services van NRB

NRB-MEDEWERKERS OPGELEID IN CYBERBEVEILIGING

Het is niet verrassend dat de NRB-groep een doelwit is voor hackers. "*Een groot deel van ons internetverkeer komt uit Rusland en China. Vandaag wordt 25% van dit verkeer nog altijd automatisch geblokkeerd omdat wij het als een potentiële bedreiging hebben geïdentificeerd. We ervaren regelmatig een aanzienlijke toename van het verkeer, wat een teken is van een inbraakpoging. Gelukkig zijn onze systemen afdoende beschermd* ", legt Lorenzo Bernardi uit.

Om deze bedreigingen tegen te gaan, moet elke medewerker verschillende beveiligingsmodules volgen. Het Quality & Risk team, onder leiding van Emmanuelle Lhermitte, is verantwoordelijk voor deze opleiding. Die maakt het personeel onder meer bewust door middel van phishingtests die elk kwartaal worden uitgevoerd. Als een willekeurig gekozen persoon in de val loopt, krijgt hij een individuele follow-up. "*Elke medewerker moet deze opleidingen volgen, afhankelijk van de behoeften van zijn functie. Elke module eindigt met een evaluatie. We doen er alles aan om de hele groep bewust te maken van het risico van hacking* ", legt Emmanuelle Lhermitte uit.

CONTACT

INFO@NRB.BE

www.nrb.be

www.linkedin.com/company/nrb

@daringtocommIT

info@nrb.be | +32 (0)4 249 72 11

NRB S.A. / nv Parc Industriel des Hauts-Sarts - 2e Avenue 65 - 4040 Herstal | Boulevard Bischoffsheim, 15 - 1000 Bruxelles / Brussel

THE NRB GROUP

bsi. ISO 9001:2015 Quality Management FS 706532 ISO/IEC 27001 Information Security Management IS 706533

Designed at NRB | 23/11/2023