
80%
DE GEMIDDELDE SCHADE LOOPT OP TOT 80 PROCENT VAN DE JAAROMZET
DE PROOI

MIDDEN-EN KLEINBEDRIJF FAVORIETE PROOI VAN CYBERCRIMINELEN

Drieënveertig procent van alle cyberaanvallen richt zich op het midden- en kleinbedrijf. Zestig procent van de getroffen ondernemers gaat binnen zes maanden failliet. Het zijn cijfers die duidelijk maken hoe kwetsbaar met name het mkb is voor cybercriminaliteit. Tegen die achtergrond kreeg het betoog van Peter Lahousse, cyberexpert en ethisch hacker, extra urgentie tijdens het VVVF-jaarevent, waar hij sprak over digitale weerbaarheid.

TEKST: ADRIAAN VAN HOOIJDONK
FOTO'S: ISTOCK / BISONDER PRODUCTIES

De bevlogen cybersecurity-expert houdt zich fulltime bezig met cybercriminaliteit en digitale veiligheid. Als oprichter van Cybercrimeinfo is Lahousse gespecialiseerd in cybercriminaliteit en opsporing op het darkweb. Sinds 2017 zet de Bredanaar zich volledig in voor het vergroten van bewustwording en het bieden van oplossingen tegen cyberdreigingen. Als onderzoeker en spreker volgt hij de razendsnelle ontwikkelingen op de voet en vertaalt hij complexe dreigingen naar begrijpelijke en toepasbare inzichten voor organisaties. Lahousse werkt samen met politie, gemeenten en bedrijven en stuurt dagelijks rapportages over actuele cyberdreigingen naar binnen- en buitenlandse veiligheidsdiensten, met als doel Nederland weerbaarder te maken tegen geopolitieke dreigingen en nieuwe cyberaanvallen.

Failliet

Cybercrime, ook wel computercriminaliteit genoemd, treft in toenemende mate het midden- en kleinbedrijf. Zo is 43 procent van de cyberaanvallen specifiek op het mkb gericht. En het loopt vaak slecht af: zestig procent van de mkb'ers die slachtoffer wordt van een ernstige cyberaanval gaat binnen zes maanden failliet, blijkt uit curatorrapporten. De kosten zijn enorm: gemiddeld loopt de schade op tot 80 procent van de jaaromzet. Elke elf seconden wordt wereldwijd een bedrijf getroffen door een ransomeware-aanval. Verzekeren is mogelijk, maar 'pas op voor adders onder het gras', waarschuwde Lahousse. Verzekeraars stellen steeds strengere eisen aan cybersecuritymaatregelen bij bedrijven en premies kunnen fors oplopen.

Kosten

Naast directe financiële schade wees Lahousse op de indirecte gevolgen van cybercriminaliteit, zoals reputatieschade, productiestilstand en personeel dat moet vertrekken. Hij verwees naar ondernemer Xander Koppelmans uit Goes, die na een hack letterlijk alles kwijtraakte. "Binnen twee jaar van zorgeloos naar dakloos." De dader bleek in China te zitten en daar was juridisch nauwelijks tegen op te treden.

Lahousse liet in een video zien hoe ransomwarecriminelen te werk gaan. Zij stelen data, zetten bedrijfssystemen op slot en eisen losgeld om de systemen weer vrij te geven. Wereldwijd loopt de schade in de duizenden miljarden euro's. Het gaat om zware, goed georganiseerde criminaliteit met een enorme maatschappelijke impact. Zo wisten cybercriminelen onlangs met één aanval honderden bedrijven tegelijk te treffen. Hun eis? "Jullie krijgen je data terug als wij 70 miljoen dollar aan bitcoins ontvangen."

MKB kwetsbaar

Vooral het mkb is kwetsbaar, bleek uit zijn presentatie. Veel bedrijven beschikken niet over gespecialiseerde IT-beveili-

The Perfect Mix

Eskens Process Solutions, Kwaliteit en Service

Sterke merken, een ervaren team en een efficiënte service
zijn de ideale mix voor een waardevol partnership

WILHELM NIEMANN
MASCHINENFABRIK

WAB

ESKENS
PROCESS SOLUTIONS

HOE CYBERCRIMINELEN SYSTEMATISCH TE WERK GAAN

Om inzicht in de werkwijze van cybercriminelen te geven, is er het Cyber Kill Chain model. Het bestaat uit de volgende zeven stappen.

1. Verkenning – het identificeren van doelwitten door informatie te verzamelen
2. Bewapening – het creëren van malware of andere tools om de aanval uit te voeren
3. Bezorging – het afleveren van de schadelijke software of exploit, bijvoorbeeld via e-mail
4. Uitbuiting – het benutten van kwetsbaarheden in het doelwit om toegang te krijgen
5. Installatie – het installeren van malware, zoals een backdoor, om controle te verkrijgen
6. Beheer en controle – het opzetten van een communicatiekanaal tussen de aanvaller en systeem
7. Uitvoeren van het doel – het behalen van het uiteindelijke doel

TIPS EN TRICKS OM DE DIGITALE WEERBAARHEID TE VERHOGEN

- Onderschat de impact niet
- Creëer bewustzijn binnen de organisatie
- Zorg dat de software up to date is
- Monitor en inventariseer kwetsbaarheden
- Stel een incidentrespons en herstelplan op

ging, terwijl cybercriminelen dankzij anonimiteit en schaalgrootte van internet relatief eenvoudig slachtoffers maken en lang buiten het zicht van opsporingsdiensten blijven. Het traceren van daders is lastig, mede omdat zij opereren vanuit andere landen. Zelfs als criminelen worden geïdentificeerd, is arrestatie vaak problematisch. De motieven variëren, maar geld verdienen en het toebrengen van schade aan bedrijven zijn de belangrijkste drijfveren.

Daarom is het essentieel om te investeren in goede beveiliging en conflicten tussen directie en IT-afdeling te voorkomen wanneer het misgaat. Lahousse wees erop dat cybercriminelen op het darkweb kant-en-klare tools kopen waarmee verouderde beveiliging eenvoudig is te omzeilen.

Cryptovaluta

De wereld van cybercrime is zowel fascinerend als verontrustend. In deze digitale schaduwwereld gebeurt van alles: van hacken, phishing en ransomware tot helpdeskfraude en illegale handel op het darkweb. Ook cryptovaluta spelen een belangrijke rol bij illegale transacties, net als complexe cyberaanvallen waarbij staten en criminelen soms samenwerken. Cybercriminelen worden steeds professioneler en gerichter; hun technieken worden geavanceerder en effectiever.

Het is een groeiend probleem dat iedereen raakt: van individuen en bedrijven tot overheden.

Gestolen data worden vaak gedeeld of verkocht op het darkweb, bijvoorbeeld om slachtoffers onder druk te zetten of extra inkomsten te genereren. De gevolgen zijn groot: emotionele schade, identiteitsfraude, financiële verliezen, reputatieschade en juridische problemen. De afgelopen jaren is een zorgwekkende stijging zichtbaar in het aantal Belgische en Nederlandse organisaties (het werkgebied van Lahousse) waarvan gegevens op het darkweb zijn gelekt.

Nep QR-codes

Volgens Lahousse kennen cybercriminelen grofweg twee aanvalsroutes: via de mens en via de techniek. Technisch gaat het vaak mis door verouderde software en ontbrekende beveiligingsupdates. Aan de menselijke kant spelen zwakke of hergebruikte wachtwoorden een belangrijke rol, net als het onzorgvuldig aanklikken van links of het openen van verdachte bijlagen. “Een e-mail is de hoofdtoegang voor een crimineel. Daar moet je goed toezicht op houden. Maar dat gebeurt niet, want we handelen onze mails snel af en hebben niet door dat achter een bestand een hacker kan schuilgaan.”

Hij waarschuwde voor het ‘valse gevoel van veiligheid’ dat tweestapsverificatie (2FA) kan geven. Moderne aanvalstechnieken zijn steeds beter in staat 2FA te omzeilen. Daarom is het noodzakelijk om 2FA te combineren met aanvullende maatregelen, zoals wachtwoordmanagers, monitoring en bewustwordingstrainingen. Ook het scannen van QR-codes vraagt om alertheid. Criminelen plakken steeds vaker nep-QR-codes over bestaande codes, bijvoorbeeld bij laadpalen, parkeermeters of openbare posters. Wie zo’n code scant, wordt ongemerkt doorgestuurd naar een valse website waar om betaling of persoonsgegevens wordt gevraagd. Soms lijkt het alsof je netjes afrekent, terwijl het geld rechtstreeks bij fraudeurs belandt.

GTA-model

“Alles wat je opslaat in wachtwoordmanagers, digitale kluizen en vergelijkbare systemen kunnen cybercriminelen kraken.” Daarom pleitte Lahousse voor een methode waarbij wachtwoorden worden berekend in plaats van opgeslagen. Zo ontwikkelde een Nederlands bedrijf een wachtwoordmanager die met een wiskundige formule unieke wachtwoorden genereert, zonder deze centraal op te slaan.

Cybercriminelen hanteren het GTA-model: geloofwaardigheid, tijdsdruk en angst (emotie). Afhankelijk van de kwetsbaarheid kiezen zij hun aanpak. Technische aanvallen verlopen vaak geautomatiseerd of handmatig, terwijl bij menselijke zwakheden sprake is van spear-aanvallen (gericht op één individu) of spray-aanvallen (breder en minder gericht). Criminelen zoeken daarbij altijd naar de zwakste schakel, die zich niet zelden bevindt bij een toeleverancier van het uiteindelijke doelwit. “Trek daarom voldoende tijd en budget uit voor gedegen beveiligingsadvies en passende maatregelen,” aldus Lahousse.

GEEN NIS2-PLICHT VOOR DE MEESTE VVVF-LEDEN, WEL TOENEMENDE CYBERSECURITY-EISEN

De Tweede Kamer behandelt in maart de Cyberbeveiligingswet, die is gebaseerd op de Europese NIS2-richtlijn voor netwerk- en informatieveiligheid. De wet treedt naar verwachting het tweede kwartaal 2026 in werking. Het grootste deel van de VVVF-leden valt niet direct onder deze wet, maar hun klanten mogelijk wel en die zullen dan ook eisen stellen aan hun leveranciers.

VVVF-leden voor wie de wet wel van toepassing is, moeten zich registreren bij het Nationaal Cyber Security Centrum. Ook moeten zij hun netwerken en systemen beveiligen en significante IT-incidenten melden. Daarvoor is een centraal meldpunt ingericht bij het Nationaal Cyber Security Centrum. “Verder moeten ze ervoor zorgen dat toeleveranciers hun cybersecurity op orde hebben en hen daarop aanspreken als dat niet het geval is”, zegt Tamara Idema, sector & regulatory affairs manager VVVF.

Samen Digitaal Veilig

Cyberaanvallen zijn een snel groeiende bron van zorg. Zo verdubbelde het aantal ransomware-aanvallen gericht op datadiefstal in 2025, waarschuwde het Nationaal Cyber Security Centrum eind vorig jaar. Om de leden te ondersteunen heeft de VVVF zich aangesloten bij Samen Digitaal Veilig, een platform van ruim honderd samenwerkende brancheorganisaties en kennis- en marktpartijen dat bedrijven weerbaarder maakt met informatie en instrumenten voor digitale veiligheid. Via het platform kunnen bedrijven zich voorbereiden op een externe audit en het NIS2 Supply Chain-certificaat behalen, om klanten, ketenpartners en andere stakeholders te laten zien dat de cyberveiligheid op orde is. Steeds vaker zijn aanvallen immers niet rechtstreeks op een bedrijf gericht, maar op leveranciers of partners, benadrukt Samen Digitaal Veilig.

Goed voorbereiden

Het is cruciaal dat bedrijven zich voorbereiden op de indirecte gevolgen van cyberaanvallen voor hun bedrijfsvoering. “De impact van stroomuitval kan enorm zijn,” waarschuwt Idema. “Blijft de productie draaien? Wat gebeurt er met de opslag van gevaarlijke stoffen of met de luchtafzuiging op de werkvloer?” Zij adviseert bedrijven hun kwetsbaarheden systematisch in kaart te brengen, regelmatig back-ups te maken en herstelprocedures te testen en te oefenen. Ook moeten scenario’s van stroom- of waterverstoring worden meegenomen in trainingen en oefeningen, en moeten medewerkers weten waar zij betrouwbare en actuele informatie kunnen vinden.

Crisisdraaiboeken

Leg daarom de communicatielijnen vooraf vast: wie verzorgt de interne communicatie en wie spreekt namens het bedrijf naar buiten? Juist in een crisissituatie, wanneer chaos dreigt, voorkomt een duidelijk stappenplan dat mensen op basis van emotie of improvisatie gaan handelen. Idema wijst er bovendien op dat cruciale contactgegevens, zoals telefoonnummers, ook fysiek beschikbaar moeten zijn, bijvoorbeeld op papier, voor het geval digitale systemen of telefoonlijsten niet meer toegankelijk zijn. Steeds meer organisaties werken inmiddels met dergelijke crisisdraaiboeken; om deze op te stellen bestaan ook hulpmiddelen bij diverse organisaties, onder meer Samen Digitaal Veilig en het ministerie van Economische Zaken.

ECO CONCEPT

Up to 100 % recycled material. 100 % spectacular.

An important step for the circular economy. Take action!

Are you ready?
Scan the QR code now and find out more about the Jokey Eco Concept!

jokey

Packaging Done Wisely.