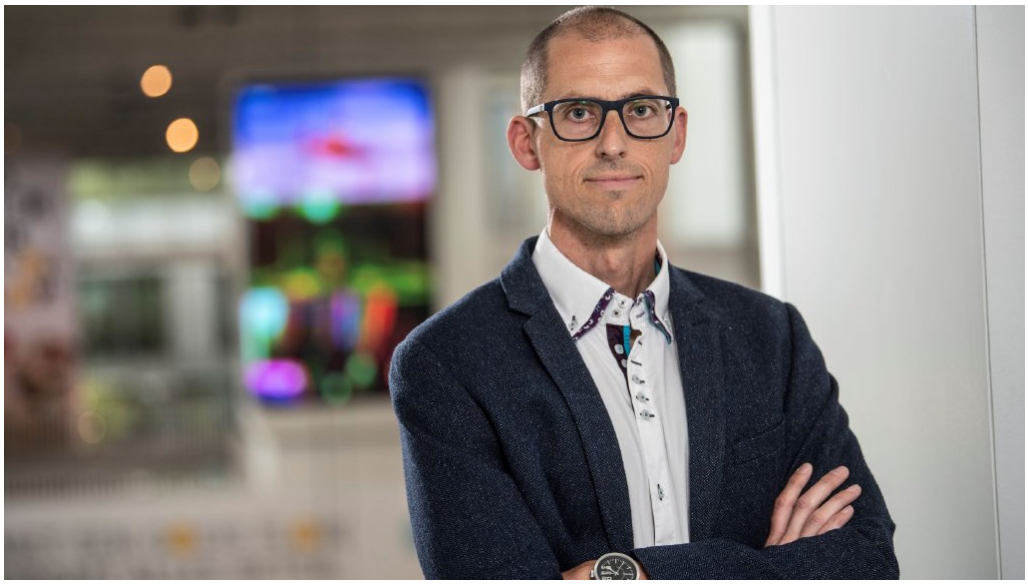
TIJD CONNECT > CYBERSECURITY

Tijd Connect biedt organisaties toegang tot het netwerk van De Tijd. De partners zijn verantwoordelijk voor de inhoud.

'De werkplek is geen burcht met een slotgracht rond'



Stefaan Wuytack, Telenet Business: 'Pure firewall-aanvallen zijn verdwenen, want die zijn tijdrovend en worden vaak onderschept.'

13 oktober 2020 07:53

Cybercriminaliteit is een industrie geworden. De hackers van vandaag zijn heuse professionals. Telenet Business staat zijn klanten bij in hun nieuwe cybersecuritybehoeften. 'Het gaat niet alleen meer om technologie, maar ook om processen en mensen.'

Tot een paar jaar geleden hadden bedrijven voldoende aan een fysieke firewall om zich te beschermen tegen cyberaanvallen. 'Wie toen zo'n hardware-oplossing liet installeren, was *safe*', zegt Stefaan Wuytack, senior strategy manager cybersecurity bij Telenet Business.

Makkelijk doelwit

'Vandaag is dat niet meer zo. Een firewall is een slotgracht die een burcht afsluit. Dat werkte in het verleden prima, maar intussen is de bedrijfswereld veranderd. De corona-uitbraak duwt werknemers richting thuiswerk. Daardoor bestaat die burcht niet meer en is er een nieuwe aanpak nodig, met onder andere een firewall die meer schaalbaar is en het nieuwe werken kan ondersteunen.'

Bedrijven denken vaak dat ze geen interessante prooi zijn voor hackers. Dat is een zware misvatting.

STEFAAN WUYTACK
SENIOR STRATEGY MANAGER
CYBERSECURITY TELENET BUSINESS

'Hackers zijn bovendien slimmer geworden. Pure firewall-aanvallen zijn verdwenen, want die zijn tijdrovend en worden vaak onderschept. De aanvallen van vandaag zijn gericht op een makkelijker doelwit: de werknemer in zijn thuiskantoor. Phishingmails zijn tegenwoordig het grootste gevaar. Hackers gebruiken daarvoor nieuwe technologieën die eenvoudig en goedkoop zijn. Vaak zijn het semiprofessionele ecosystemen, waarin de ene partij malafide software ontwikkelt en de andere partij aanvallen uitvoert.

Spear phishing

Cybercriminelen mikken op de zwakste schakel: de mens. Hierdoor ligt in negen op de tien gevallen het gedrag van een medewerker aan de basis van een beveiligingsincident.

'Om onze medewerkers bewust te maken van het gevaar, sturen we hen zelf gesimuleerde phishingmails', zegt Stefaan Wuytack. 'Helaas zetten hackers steeds vaker in op een nieuwe variant: *spear phishing*. Daarbij worden op basis van artificiële intelligentie persoonlijke gegevens van het internet geplukt en gebruikt in een gerichte en professioneel uitziende e-mail.'

Zware misvatting

Telenet Business helpt bedrijven in hun strijd tegen cybercriminaliteit. Stefaan Wuytack stelt vast dat nogal wat bedrijven ervan uitgaan dat ze niet interessant genoeg zijn voor hackers.

De tijd van de e-mails van Nigeriaanse prinsen in

'Dat is een zware misvatting. Phishing betekent letterlijk: een net uitgooien en wachten tot iemand daarin terechtkomt. Dat kan eender wie zijn. De

schabouwelijk Engels is voorbij.

STEFAAN WUYTACK
SENIOR STRATEGY MANAGER
CYBERSECURITY TELENET BUSINESS

technologische evolutie brengt spear phishing binnen handbereik van hackers. De tijd van de e-mails van Nigeriaanse prinsen in schabouwelijk Engels is voorbij.'

Security officer

De evolutie inzake cybercriminaliteit heeft gevolgen voor de jobinhoud van de security officer. Beveiliging draait niet meer louter om technologie, maar ook om mensen en processen. Een security officer moet van veel markten thuis zijn.

'Omdat je als onderneming onmogelijk alle competenties en middelen in huis kan hebben, is samenwerken met een betrouwbare partner essentieel', stelt Stefaan Wuytack. 'Telenet Business biedt schaalbare oplossingen op maat van elk bedrijf.'

Weerbaarheid

'Wij houden bedrijven een spiegel voor om hun weerbaarheid te testen. Cybersecurity draait om het besef dat een geslaagde aanval slechts een kwestie van tijd is. En als je aangevallen wordt, komt het er op aan om die aanval zo snel mogelijk te detecteren en daadkrachtig te reageren. Zo blijft de operationele impact minimaal en is de continuïteit van de business verzekerd.'

'Je kan altijd ziek worden, maar het is je weerstand die bepaalt hoe ziek je wordt. Zonder die weerbaarheid is investeren in cybersecurity een druppel op een hete plaat.'

Naar meer weerbaarheid tegen cyberaanvallen

Gerichte cyberaanvallen vormen een reële dreiging met potentieel grote gevolgen voor de continuïteit van bedrijven. Een oplossing die beschermt tegen àlle soorten dreigingen bestaat echter niet.

Wie zich maximaal wil wapenen tegen digitale indringers, doet dat in de eerste plaats door de impact van een aanval te verkleinen.

LEES VERDER

CYBERSECURITY: TELENET BUSINESS

Hoe beschermt u zich tegen grote netwerkaanvallen?

Steeds meer bedrijven worden het slachtoffer van een grote netwerkaanval of DDoS-aanval. Daarbij worden hun systemen bestookt met grote hoeveelheden data vanuit het internet, waardoor hun systemen verzadigd

CYBERSECURITY: TELENET BUSINESS

'U detecteert een cyberaanval best voor u geraakt wordt'

Terwijl bedrijven door het vele telewerk kwetsbaarder dan ooit zijn, worden hackers steeds professioneler. Zich louter wapenen tegen cyberaanvallen volstaat niet meer. Een snelle detectie en een goed actieplan zijn

CYBERSECURITY: TELENET BUSINESS

Wat te doen als uw bedrijf gegijzeld wordt via het web?

Ransomware gijzelt bestanden of computers tot het slachtoffer 'losgeld' betaalt. Willem Janssens, cybersecurity expert bij Telenet Business, legt uit hoe bedrijven zich hiertegen kunnen wapenen.

CYBERSECURITY: TELENET BUSINESS

Anders werken vraagt om aangepaste beveiliging

Bedrijven werken volop in de cloud en stappen massaal over naar telewerk. Dat maakt hen kwetsbaarder voor cyberaanvallen. 'Vandaag hebben bedrijven een totaaloplossing nodig.'

CYBERSECURITY: TELENET BUSINESS

Thuiswerk vergt een nieuwe beveiligingsaanpak

Het coronavirus verplicht bedrijven om halsoverkop over te schakelen naar thuiswerk. Die omschakeling houdt heel wat uitdagingen in, vooral op het vlak van cybersecurity. Telenet Business ondersteunt zijn …

- Hoe beschermt u zich tegen grote netwerkaanvallen?
- Wat te doen als uw bedrijf gegijzeld wordt via het web?
- Anders werken vraagt om aangepaste beveiliging
- 'U detecteert een cyberaanval best voor u geraakt wordt'
- Thuiswerk vergt een nieuwe beveiligingsaanpak