Motiv vestigt aandacht op pijnlijke gevolgen cyberdreigingen

door Ferry Waterkamp, freelance ICT-journalist

Motiv organiseerde begin maart in De Olifant in Breukelen een updatesessie over de gevaren van cyber dreigingen en hoe organisaties zich hiertegen kunnen wapenen. Tijdens discussies met de zaal kwam de aandacht al snel te liggen op `de mens` als de zwakste schakel en het belang om alert te zijn op social engineering. "Slechts twee muisklikken kunnen verstrekkende gevolgen hebben", zo merkte Pre-Sales Security Engineer Niels den Otter van Check Point Software Technologies op.

De sessie werd geopend door ICT-journalist Brenno de Winter die de afgelopen jaren bekendheid verwierf door kwetsbaarheden bloot te leggen in de beveiliging van onder andere de ov-chipkaart, DigiNotar en KPN. Als onderdeel van de actie 'Lektober' schoot hij gaten in een vijftigtal gemeentewebsites. "Niet omdat ik een hekel heb aan gemeentes, maar omdat ik vind dat je als gemeente de plicht hebt om een minimale beveiligingsstandaard te hanteren. Als burger ben je namelijk verplicht om je gegevens bij een gemeente achter te laten."

Tijdens zijn presentatie probeerde De Winter de ogen van het publiek te openen door te wijzen op de mogelijk catastrofale gevolgen van het niet goed op orde hebben van de beveiliging. "DigiNotar was twee weken na het bekend worden van het beveiligingsincident failliet. DigiNotar had dan ook mensen in gevaar gebracht door na de inbraak vol te blijven houden dat 'alles oké' was." Maar ook het lekken van wachtwoorden via een gemeentewebsite kan verstrekkende gevolgen hebben als de eigenaar van een wachtwoord hetzelfde wachtwoord ook op andere plaatsen gebruikt. "Gelooft u mij, ik word niet graag geconfronteerd met berichten die ik tien jaar geleden heb achtergelaten op een datingsite", zo gaf De Winter als voorbeeld. "Er zijn voorbeelden van mensen die hun baan hebben opgezegd en iets anders zijn gaan doen, gewoon omdat de situatie te pijnlijk was."

"Retentie is ontzettend belangrijk", zo drukte De Winter het publiek op het hart. "Gooi je verouderde data weg, dan heeft een lek ook minder impact. Het scheelt nogal of er na een lek de gegevens van 30 of 30.000 personen op straat komen te liggen."

Cyber Security

Bastiaan Bakker, Directeur Business Development bij Motiv, ging tijdens zijn presentatie dieper in op de maatregelen die organisaties kunnen nemen tegen cyberdreigingen. Hij onderscheidde daarbij drie fasen die moeten leiden naar een volwassen vorm van Cyber Security. De eerste fase bestaat uit het optimaliseren van de weerbaarheid met behulp van moderne technologieën en het plaatsen van beschermende maatregelen. "Voorkomen is nog altijd beter dan genezen", merkte Bakker op. De tweede fase bestaat uit het inrichten van security monitoring – eventueel binnen een Cyber Security Operations Center – om inbraken en gedrag te kunnen 'signaleren en filmen'. De derde stap is het beperken van de schade door het inrichten van een incident- en response-team dat als een soort mobiele brandweer kan uitrukken als het nodig is.

"Maar het op orde krijgen van dit proces neemt zeker drie jaar in beslag", merkte Bakker op. "De camera's moeten eerst op de juiste plek worden opgehangen en de alerting moet op de juiste manier zijn ingeregeld; pas dan heeft het zin om de mobiele brandweer uit te laten rukken.

En dan nog zijn we alleen maar reactief bezig. We moeten naar een proactieve aanpak door gebruik te maken van de security intelligence die wereldwijd beschikbaar is. Hier zijn we in Nederland nog nauwelijks mee bezig. De rol van Motiv is om tussen de klant en de 'Cyber Intelligence' in te gaan zitten, door het collecteren en analyseren van de informatie, het formuleren van een boodschap en het uitvoeren. Motiv kan functioneren als de lokale hub richting dat internationale speelveld."

> `We moeten naar een proactieve aanpak door gebruik te maken van de security intelligence die wereldwijd beschikbaar is`

Gebruikers centraal

De presentatie van Bakker wierp vanuit het publiek al snel de vraag op of een Cyber Security-aanpak zich niet in eerste instantie moeten richten op 'security awareness' en het 'opvoeden' van de gebruikers? Algemeen wordt immers aangenomen dat social engineering de primaire methode is om malware op machines geïnstalleerd te krijgen die dan op afstand kunnen worden overgenomen. "Je kunt technisch alles op orde hebben, maar als de gebruikers niet alert zijn op social engineering fiets je zo door de beveiliging", merkte een bezoeker op.

"Social engineering is al zo oud als de weg naar Kralingen, alleen gaat het nu via wegen als LinkedIn en Facebook", bevestigde Niels den Otter van Check Point tijdens zijn presentatie. "De mens is van nature nieuwsgierig en dat is meteen het eerste probleem. Een e-mail wordt eerst aangeklikt en pas daarna wordt nagedacht over de mogelijke gevolgen. Slechts twee klikken kunnen zo verstrekkende gevolgen hebben."

Demonstratie

De dag in Breukelen werd afgesloten met een demonstratie van Crossbeam's high-performance hardwareplatform dat is geoptimaliseerd voor het draaien van de beveiligingssoftware van derde partijen zoals Check Point en Imperva.

Met dit platform is het volgens de leverancier mogelijk om zaken als firewall, IDS, IPS, URL-filtering en antimalware te consolideren binnen één chassis zonder in te boeten op performance. Als de verschillende beveiligingsapplicaties op verschillende appliances worden gedraaid is vaak wel sprake van een aanzienlijk performanceverlies, zo stelde Zach Barile, bij Crossbeam Director Global Alliances. "Door de consolidatie kun je de applicaties bovendien integraal monitoren op de gezondheid."

Al met al kan worden teruggekeken op een geslaagd evenement dat bij de bezoekers een behoefte heeft ingevuld. "Ik ben hier naartoe gekomen om me te oriënteren op voor mij nieuwe ontwikkelingen en Crossbeam kende ik nog niet", reageert Ed Voncken, consultant van CVIS en een van de meer dan 80 aanwezigen. "Steeds meer zaken worden via internet afgehandeld maar in de top van organisaties is nog te weinig het bewustzijn dat je dan je Cyber Security op orde moet hebben. Dat bewustzijn komt vaak pas nadat de organisatie is gehackt. Dat wil ik graag voor zijn." ●●

Op donderdag 19 april 2012 organiseert Motiv een Security in Mobiliteit updatesessie. Na de zeer succesvolle Cyber Security-updatesessie van afgelopen maart, staat deze tweede updatesessie van 2012 in het teken van Security in Mobiliteit.

Samen met een aantal toonaangevende en internationaal georienteerde partners, waaronder Juniper en SecurEnvoy geven wij u meer inzicht in het belang van securityvraagstukken binnen de wensen als telewerken, de 24-uurs economie en Het Nieuwe Werken. Naast de presentaties door externe sprekers, partners en Motiv is deze sessie, zoals u gewend bent, uiterst interactief. Wij hebben tijdens de voorbereiding van dit evenement van een aantal relaties het verzoek gehad om ook in te gaan op onderwerpen mobile device management en lifecyclemanagement van mobiele devices.

19 april: MOTIV PRESENTEERT HET BELANG VAN SECURITY IN MOBILITEIT VOOR U EN UW ORGANISATIE!

Wij stellen uw aanwezigheid zeer op prijs! Inschrijven kan nu!