Wim de Graaf (l) en Eric Klomp (r) zijn werkzaam bij Entris in Ede en ondersteunen ondernemers onder andere bij databeveiliging.

CYBERCRIME

ONZICHTBAAR GEVAAR VOOR ICT-OMGEVING

Volgens Symantec werden vorig jaar 3,4 miljoen Nederlanders slachtoffer van cybercrime. Ze raakten in totaal 1,3 miljard euro kwijt. Vallei Business stelde Eric Klomp (operationsmanager) en Wim de Graaf (salesmanager), beiden werkzaam bij ICT-specialist Entris in Ede, een aantal prangende vragen over het onzichtbare gevaar voor de ICT-omgeving. Entris is onderdeel van Lagarde Groep, bestaande uit Lagarde, Entris, Blankestijn Beveiliging, Escron en Excellis.

WAT IS DE GROOTSTE MISVATTING OVER DE BESCHERMING TEGEN CYBERCRIMINALITEIT?

Klomp: "Bij organisaties wordt er vaak vanuit gegaan dat SAAS omgevingen zoals Microsoft Office 365, Google G-suite (en anderen), allemaal standaard goed beveiligd zijn en er geen maatregelen nodig zijn om hier beveiliging toe te voegen. Dit is een grote misvatting: Een publieke cloud oplossing is niet automatisch heel sterk beveiligd. Natuurlijk zijn er bij de grote cloud providers sterk ingeregelde firewalls aanwezig die veel verkeer niet toestaan, echter zodra je een server in bijvoorbeeld Azure aanschakelt dan weet je dat je direct wordt aangevallen. Als het gebruikersbeheer dan niet goed geregeld is (bijvoorbeeld met een eenvoudig wachtwoord en geen multi-factor authenticatie), dan komen de cybercriminelen alsnog eenvoudig binnen zonder dat iemand dit in de montoring ziet (het is gewoon een gebruikersaccount wat dan binnenkomt en dat wordt toegestaan)."

DUS GAAT HET IN DE PRAKTIJK VAAK MIS BIJ ONDERNEMERS?

Klomp: "Het risico voor de Nederlandse mkb'ers is erg groot. Voorbeelden hiervan hebben we genoeg gezien. Iedereen is verzekerd tegen brand (verplicht voor hypotheek), maar bij cybercriminaliteit is het anders: het is een onzichtbare dreiging: de mkb'ers verwachten dat het niet bij de mkb'ers zelf zal plaatsvinden, dus hoeven hier niets aan te doen: het is onzichtbaar. Het probleem hoeft niet groot te zijn, als de voorbereidende maatregelen maar voldoende zijn om aanvallen af te weren of als er dan toch een aanval door komt, de data beveiliging goed geregeld is middels back-ups (of versions). De Graaf: "En daar zit wel een knelpunt. Als de kans nihil wordt ingeschat is men niet altijd bereid preventief te investeren in beveiliging."

OP WELKE MANIER HELPT ENTRIS BIJ DATABEVEILIGING VAN ONDERNEMINGEN?

Klomp: "Entris helpt ondernemingen bij de databeveiliging door diverse technische maatregelen, echter mist vaak een stuk awareness bij de gebruikers. De gebruikers zijn regelmatig de zwakste schakel in het geheel, waardoor de technische maatregelen nog zo goed kunnen zijn, maar de cybercrimineel door de beveiliging heen wordt gebracht door de gebruikers zelf. Entris ondersteunt de bedrijven door technisch en organisatorisch te kijken naar de getroffen en te treffen maatregelen. Entris kan tevens een awareness sessie organiseren, waarbij met voorbeelden wordt getoond hoe eenvoudig het kan zijn dat cybercriminelen toegang

'HET ACHTERLOPEN OP UPDATES IS VRAGEN OM MOEILIJKHEDEN'

krijgen. Naast deze maatregelen zorgt Entris voor de databeveiliging in de vorm van rechten instelling (gebruikers alleen rechten geven op delen waar ze rechten moeten hebben) maar ook door toetsing van het beveiligingsbeleid (jaarlijks) volgens onze ISAE3402 Type II norm: jaarlijkse controle van het beveiligingsbeleid."

ENTRIS KAN EEN INTERNE SCAN MAKEN, WAT HOUDT DEZE SCAN PRECIES IN?

Klomp: "De interne scan zorgt ervoor dat er inzicht komt in de technische staat van de beveiliging. Dit gaat zowel van binnen-uit als van buitenaf. Naast deze technische scan houden we interviews (niet alleen met de ICT manager, maar zeker ook met gebruikers) om te reviewen waar de beveiling staat in ons opgestelde security framework. In het eindrapport komen adviezen vanuit Entris: wat te doen om op een hoger security niveau te komen. De scan verkent niet alleen het netwerk, maar ook de Active Directory en voert een zogenaamde 'best practice'-scan uit, waaruit moet blijken of geen 'gaten' in onder andere het security beleid van Active Directory zitten. Dit wordt uiteindelijk naast de interviews gelegd, ter controle of wat gezegd wordt ook is ingeregeld (hier zit soms nog wel een verschil in). De Graaf vult aan: "Het voordeel van deze aanpak is dat de klant inzichtelijk heeft waar hij staat. Hij maakt zelf de beslissing welke stappen ook daadwerkelijk worden uitgevoerd."

ZIJN ONDERNEMERS VAAK VERBAASD OVER DE UITKOMST?

Klomp: "Bij een groot aantal van onze klanten wordt regelmatig een security scan gehouden. Een groot aantal mkb'ers weten wel dat er security risico's zijn, echter voordat er actie ondernomen wordt kan het soms al te laat zijn. Omdat het onzichtbare dreiging is, is het erg lastig om mkb'ers te overtuigen dat er daadwerkelijk risico's zijn. Dreigingen komen regelmatig uit verschillende hoeken, waardoor het voor ondernemers vaak lastig is om altijd op tijd de juiste maatregelen te nemen. We zien de laatste tijd dat er bijvoorbeeld Microsoft Office 365 accounts worden overgenomen (via phishing-methode." "Als cybercriminelen toeslaan is er vaak al wat aan vooraf gegaan", voegt De Graaf toe. "Het is dan ook niet altijd toereikend om de backup van een week eerder terug te zetten. De infiltratie kan al maanden eerder in gang zijn gezet."

IS DATABEVEILIGING ALLEEN VOLDOENDE OM JE GEGEVENS TE BESCHERMEN?

Klomp: "Natuurlijk zijn de databeveiligingsmaatregelen noodzakelijk om de zaken goed af te schermen (lees brandverzekering is afgesloten), maar de awareness is een factor die nog veel belangrijker is. Als je een brandverzekering hebt afgesloten ben je niet verzekerd tegen het feit dat er nooit brand uit breekt. Dat moet je dan nog zelf voorkomen (je gaat geen vuurkorf in de woonkamer branden). Dit geldt ook voor beveiliging; Je account kent een complex wachtwoord met relatief veel karakters (liefst rond de 12) en je gebruikt two-factor authentication om in te loggen (een account, een wachtwoord en een apparaat waar een code op wordt gegenereerd zoals bijvoorbeeld je telefoon). Zodra gebruikers zien hoe eenvoudig het is om schade aan te richten zodra het account bekend is, wordt de awareness groter. Dit zijn sessies die we bij Entris graag organiseren en laten zien."

IS HET OPZIJ ZETTEN VAN DE PRIVACY VAN MEDEWERKERS DE OPLOSSING IN DE STRIJD TEGEN CYBERCRIMINALITEIT?

Klomp: "Er blijft altijd een strijd tussen privacy en cybercriminelen. De vraagstelling die hier staat is een hele lastige en is meer een morele keuze. De privacywetgeving gaat hierbij de medewerkers al enigszins beschermen. Ik ben van mening dat cybercriminelen moeten worden gestopt, ook als dit ten koste gaat van de privacy van de medewerkers. De schade door cybercriminelen kan zo groot zijn, dat een bedrijf dit niet overleefd. Dan is de schade voor de medewerkers nog groter."

WELKE TIPS ZOUDEN JULLIE ONDERNEMERS MEE WILLEN GEVEN WANNEER ZIJ ZICH WILLEN WAPENEN TEGEN CYBERCRIMINALITEIT?

Klomp: "Het wapenen tegen cybercriminaliteit is niet een eenmalige actie: een project draaien en dan zijn we beschermd is geen oplossing. Zorg ervoor dat de awareness bij de gebruikers zo hoog mogelijk is en laat dit in het bedrijfsproces opnemen. Dit kan bijvoorbeeld door tijdens algemene overleggen bij ieder overleg even de security te benoemen met de huidige risico's (wisselende plaatsen waar het risico vandaan komt). Doe naast de awareness een jaarlijkse scan op de status van de techniek: is die volledig opgewassen tegen cybercriminaliteit en waar zitten nog de risico's. De Graaf: "Draai waar mogelijk mee met de updates van leveranciers. Het achterlopen op updates is vragen om moeilijkheden."