tekst: Marlies Dinjens

TOTAALLEVERANCIER OP HET GEBIED VAN ICT

Het beschermen van persoonsgegevens en data door mkb-bedrijven is een hot topic merkt Tosch Automatisering & Security. IT-security levert spannende verhalen op met verdwenen miljoenen, maar het bedrijf uit Barneveld is uitgegroeid tot totaalleverancier op het gebied ICT-dienstverlening.

Twintig miljoen euro wisten cybercriminelen in een periode van anderhalf tot twee jaar tijd op slinkse wijze weg te sluizen bij een relatie zonder dat dit opviel. Op het moment dat de roof ontdekt werd was het geld spoorloos verdwenen en kon de instelling er naar fluiten. Het klinkt als een heel slechte film, maar deze vorm van cybercriminaliteit waarbij bedrijven opgelicht worden is helaas aan de orde van de dag. “Natuurlijk is het deze digitale roof uitzonderlijk vanwege het enorme bedrag”, legt Daan Morren van Tosch Automatisering & Security uit Barneveld uit. “Maar de manier waarop de cybercriminelen te werk gingen is helaas gemeengoed in het bedrijfsleven.”

Tosch werd door een partner gevraagd om uit te zoeken hoe dit kon gebeuren en wat de zwakke plekken waren in de organisatie op het gebied van digitale beveiliging. Het was een heel grote klus die Tosch met een aantal partners voor de klant heeft geklaard in het afgelopen jaar. “Hackers hebben het acceptatieproces van de klant tot in het kleinste detail bestudeerd. Het was een minutieuze analyse van alle stappen in het betaalproces. Vervolgens hebben ze alle benodigde zaken om zelf betalingen goed te laten keuren in het acceptatieproces gehackt. En zo konden ze in die periode tal van betalingen van een aantal ton uitvoeren. Dit viel niet op omdat het onze klant heel veel van dit soort betalingen van

deze omvang uitvoert", vertelt Morren. Dat de sporen vakkundig werden uitgewist spreekt voor zich. Inmiddels heeft de klant maatregelen genomen, vertelt Morren. Maar hun 20.000.000 euro zien ze helaas niet meer terug.

TOTAALLEVERANCIER ICT

Tosch uit Barneveld is niet alleen specialist op het gebied van IT-security via de drie pijlers preventie, detectie en reactie. Ook biedt het bedrijf diensten als VOiP-telefonie (bellen via het internet), werken in de cloud en systeem- en netwerkbeheer. Daarmee is Tosch totaalleverancier op het gebied ICT-dienstverlening aan mkb-bedrijven. "In 1999 is Erik Top begonnen met Tosch. We werkten toen voor klanten die we tot op de dag van vandaag nog steeds volledig ontzorgen op gebied van ICT", legt Morren uit. In de loop der jaren breidde het bedrijf niet alleen haar werknemersbestand en klantenkring uit, maar werd het palet aan producten en diensten ook uitgebreid. Tosch startte met inrichten van werkplekken, automatisering en het verzorgen van het netwerk, maar levert inmiddels ook clouddiensten en VOiP-telefonie. In 2009 zette Tosch de tak van IT-security op en sindsdien werken er 'ethische hackers' in Barneveld om klanten te helpen met hun digitale beveiliging. "Onze klanten zetten ons in om de ICT geheel of gedeeltelijk te outsourcen", zegt Morren.

ONDERSCHEIDEND

De reden dat veel mkb-bedrijven kiezen voor Tosch is de combinatie van een focus op veiligheid en de technische invulling daarvan. "Veel mensen kennen bedrijven als Fox IT en Hoffmann bedrijfsrecherche, maar de lat ligt hoog om deze partijen in te huren. Eigenlijk werken zij alleen voor de echt grote bedrijven. Wie ons inhuurt krijgt beide, want we hebben expertise op het gebied van IT-security en we kunnen achterhalen hoe een cybercrimineel te werk is gegaan. Tevens zijn wij ook gecertificeerd om digitaal forensisch onderzoek uit te mogen voeren. Hiervoor is ons personeel speciaal getraind en zijn we volledig gescreend door justitie. Er zijn weinig bedrijven die werken voor de mkb-sector die dat kunnen", vertelt Morren. Tosch werkt voornamelijk voor klanten uit het mkb die gevestigd zijn in de Vallei en de Randstad. Morren legt uit dat dit bedrijven zijn met drie tot tweehonderd werkplekken. Het bedrijf uit Barneveld werkt veel voor accountants en advocatenkantoren. Dit soort bedrijven hecht volgens Morren veel waarde aan het goed beveiligen van hun data en het beschermen van persoonsgegevens. "Wat wij voor al onze klanten doen, en dat maakt ons echt onderscheidend van concurrenten, is de klantgerichtheid. Het klinkt als een open deur, maar wij werken met een vast aanspreekpunt per klant. Zodoende kan de klant met alle vragen terecht bij een van onze collega's."

'WERKNEMERS ZIJN GEVOELIG VOOR SOCIAL ENGINEERING EN PHISING'

"Wat wij voor al onze klanten doen, en dat maakt ons echt onderscheidend van concurrenten, is de klantgerichtheid."

LEZINGEN

Morren legt uit dat Tosch al meer dan tweehonderd keer gevraagd is voor lezingen en om te spreken op congressen voor ondernemers. "Zo waren een collega en ik een keer in Rotterdam voor een lezing over cybersecurity. Wat het publiek niet wist was dat wij het aanwezige wifinetwerk afluisterden. Met behulp van intelligente tools hebben we tijdens de lezing al het dataverkeer over het netwerk geanalyseerd. Op basis van deze analyse hebben we een aantal mensen uit het publiek live geconfronteerd met beveiligingsissues. Zo pakten wij er één meneer uit waarvan we al zijn inloggegevens hadden ondervangen. Onder andere van zijn domoticasysteem thuis waardoor wij zijn volledige huis in beheer hadden." Morren en zijn collega deden dit uiteraard niet om de man een hak te zetten maar om het publiek te tonen hoe makkelijk het is om gegevens te stelen en daarmee ook echt kwaad te kunnen doen. "Uiteraard zijn we later met deze meneer in gesprek gegaan om hem tips te geven over zijn beveiliging", vertelt Morren.

ETHISCHE HACKERS

In 2009 startte Tosch met de dienst van IT-Security en sindsdien groeit deze tak hard. Het draait daarbij om preventie, detectie en reactie, legt Morren uit. De 'ethische hackers' van Tosch voeren scans uit om te zien of er beveiligings- of datalekken zijn bij bedrijven. Bedrijven willen immers graag weten in hoeverre ze kwetsbaar zijn voor digitale aanvallen. Niet alleen de hardware is belangrijk ook de mens is een aspect dat wordt meegewogen door Tosch. "Werknemers zijn gevoelig voor social engineering en phising. Op die manier peuteren criminelen gevoelige informatie los bij een bedrijf met als doel om een misdaad te plegen." Morren geeft een voorbeeld: "Zo kan een receptionist het emailadres van een directielid verstrekken middels een simpel telefoontje. In combinatie met persoonlijke gegevens van dit directielid uit openbare bronnen kan via spoofing uit zijn naam via zijn mailadres een valse email verstuurd worden. Niemand die ziet dat het een fake mailadres is. Het enige dat je hier tegen kunt doen is het creëren van bewustwording." Naast technische oplossingen zijn ook beleids- en gedragsaanpasssingen vaak noodzakelijk. Bijvoorbeeld tweetraps verificatie bij het uitvoeren van een betaalopdracht.

COLLEGA'S GEZOCHT

Om al het werk aan te kunnen heeft het team van Tosch nieuwe collega's nodig, legt Morren uit. "De markt voor ict'ers is zeer krap en ook aan onze mensen wordt volop getrokken. Dus goede ict'ers zijn welkom." Om de kans op nieuwe collega's te verhogen heeft Tosch zelf 2.500 euro tipgeld over.

www.tosch.nl