Tekst: Hans Eberson

JDS BEDRIJFSAUTOMATISERING BV SERIEUZE SPELER IN DIGITALE VEILIGHEID

"IEDEREEN IS KWETSBAAR"

Wie tegenwoordig het nieuws volgt, ziet dat er steeds vaker meldingen zijn van digitale aanvallen op overheden, bedrijven en particulieren. Als je bedenkt dat alleen de uitzonderlijke gevallen het nieuws halen, zou duidelijk moeten zijn dat cybersecurity in het bedrijfsleven bovenaan de agenda zou moeten staan, want de gevolgen van een hack zijn enorm. Dat is volgens ethical hacker Jeffrey Kosman van JDS bedrijfsautomatisering bv uit Venray zeker niet het geval. "De urgentie ontbreekt. 'We hebben antivirussoftware en een firewall, wij zijn veilig', dat is de gedachte. Tot het fout gaat. En het gaat fout als je geen maatregelen neemt, kwestie van tijd."

Jeffrey Kosman heeft inmiddels tientallen opleidingen in ICT-omgevingen achter de rug. De laatste als ethical hacker bij een opleidingsinstituut in Eindhoven. "Omdat mijn werkgebied me enorm interesseert en ik het vergroten van mijn kennis als een sport zie. Tegenwoordig vooral digitale veiligheid, want op dat gebied moet er nog veel gebeuren. Om te beginnen moet de bewustwording onder bedrijven worden vergroot. Ze worden gegarandeerd tientallen keren per dag aangevallen, meestal zonder gevolgen. Maar als het een keer raak is, dan is het meteen ook goed mis."

MANAGED SERVICE PROVIDER

JDS bedrijfsautomatisering bv besteedt bijzonder veel aandacht aan de nieuwste ontwikkelingen op het gebied van veiligheid. "Omdat er elke dag nieuwe ontwikkelingen zijn die we via allerlei informatiebronnen volgen. JDS is een zogeheten Managed Service Provider (MSP), aangesloten bedrijven maken dus gebruik van onze IT-diensten. Dat betekent automatisch dat onze beveiliging perfect in orde moet zijn en dat is ook zo, daar zijn we 24 uur per dag mee bezig. Het grootste gevaar ligt echter niet hier, maar ligt in de laptops, IoT-apparaten, werkstations of smartphones van de bedrijven zelf. Hoe vaak zit een medewerker ergens langs de snelweg bij een kop koffie niet op een onbeveiligd wi-fi-netwerk, wie maakt er in het bedrijf gebruik van welke computer, gaat de laptop mee naar huis en kan een medewerker daar zelf apps op downloaden? Of hoe zit het met beveiligingscamera's, of andere IoT-apparaten, zijn die afgeschermd? Het merendeel is dat niet. Het zijn allemaal mogelijkheden voor hackers om in een bedrijf binnen te komen. Als ze eenmaal binnen zijn, hebben ze alle tijd om rustig rond te kijken, bijvoorbeeld alle interessante (klant)gegevens te kopiëren of rekeningen te plunderen, gewoon te doen waar ze zin in hebben. Soms zijn ze al maanden in een systeem binnen voor ze toeslaan."

BEWUSTWORDING

JDS bedrijfsautomatisering bv gaat heel ver in preventie. "Cybercrime is tegenwoordig een bedrijfstak met hoge rendementen. Op allerlei internetfora circuleren bijvoorbeeld gewoon databases met wachtwoorden, die zijn te koop voor elke kwaadwillende. Ons werk begint ermee bewustwording bij bedrijven te kweken, om op alle niveaus duidelijk te maken welke risico's ze lopen. We vertellen ze wat ze ter bescherming kunnen doen, hoe ze hun veiligheidsprotocollen kunnen aanscherpen. Wij beschikken ook over manieren om wachtwoordmanagement vorm te geven, zodat apparaten moeilijker te hacken zijn. We leren klanten te denken volgens het 'zero trust' principe, vertrouw niets en niks, want geen enkel object – koelkast, auto, camera, telefoon - is veilig. Bovendien maken we noodplannen voor onze klanten. Als het bij een bedrijf dan toch misgaat, je wordt gehackt, hoe, wat, waar en door wie wordt actie ondernomen? Wat kunnen we doen om alles weer ze snel mogelijk werkbaar te maken? Noem het maar een crisisplan in geval van een hack, je hebt dan in elk geval nagedacht over wat je in dat geval te doen staat. Ten slotte toch nog maar een keer het advies: neem digitale veiligheid serieus. Zorg dat je je bewust wordt van de risico's en onderneem actie, in plaats van achteraf stappen te moeten nemen om te redden wat er te redden valt."

www.jds.nl