Motiv Proactive Security Test (PST) wijst 4Some op kwetsbaarheden

"Iedere ondernemer heeft iets te verdedigen"

Ard-Jan Starrenburg – Technisch Directeur 4Some

4Some Technisch Beheer BV wist dat ze de security 'best goed' op orde hadden. Maar is 'best goed' goed genoeg? Of zijn er kwetsbaarheden waar het bedrijf zich niet van bewust is? Om deze reden deed 4Some de Proactive Security Test (PST) van Motiv. Dit is een snelle, laagdrempelige en kosteneffectieve security assessment voor het MKB. "We zijn op enkele kwetsbaarheden gewezen waarvan we het bestaan niet kenden. Daarnaast zijn we ons nu veel meer bewust van de risico's van zaken waarvan we eigenlijk wel wisten dat we ze konden verbeteren. Het rapport biedt ons concrete handvatten om te verbeteren."

Technisch beheerder 4Some heeft 80 medewerkers in dienst, waarvan het merendeel als monteur onderweg is. Vanwege de specifieke aard van de werkzaamheden heeft het bedrijf een maatwerk ERP-applicatie ontwikkeld, die op afstand met een mobiel apparaat toegankelijk is. Naast ERP en de bekende Office-applicaties werkt het bedrijf ook nog met enkele applicaties die alleen op kantoor te benaderen zijn.

Ard-Jan Starrenburg is technisch directeur van 4Some en tevens deeltijd applicatie- en systeembeheerder. "Ik doe de eerstelijns support en ik bedenk de ontwikkelrichting van ons ERP-pakket. Tweedelijns support en applicatieontwikkeling huren we bij externe ICT-dienstverleners in."

Weinig focus op procesmatige en menselijke kant van security

Security staat als belangrijk aandachtspunt op de agenda, zegt Starrenburg. Hij vertelt: "Als ik eerlijk ben, waren we primair gericht op de buitenkant: een firewall, het scannen van binnenkomende e-mailen het trouw patchen van al onze applicaties. De gedachte was: als je de voordeur goed op slot doet, wordt het voor kwaadwillenden al een stuk lastiger om binnen te komen." Hij realiseert zich wel dat alleen het beveiligen van de buitenkant niet genoeg is. "We nemen ook wel maatregelen om de binnenkant te beveiligen, maar er ligt toch net wat minder focus op", zegt hij eerlijk.

Daarnaast wist hij eigenlijk ook wel dat security meer is dan het op orde hebben van de techniek, maar investeren in een gedegen beleid deed 4Some naar zijn zeggen te weinig. "We hadden nog niet echt de focus op het belang van goede procedures op verschillende vlakken. En ook op het gebied van awareness konden we verbeteren."

Laagdrempelige en onafhankelijke test

Die gevoelens op de achtergrond kwamen naar de voorgrond toen hij een bezoek bracht aan zijn klant Motiv. "Wij beheren voor hen alle technische installaties. Ze zijn al jarenlang klant bij ons, we hebben een goede relatie. Dus we praten ook wel eens over hun business. Zodoende hoorde ik over de PST. Omdat de dreigingen, zeker van ransomware aanvallen, toenemen, heb ik gezegd: kom die test ook maar eens bij ons uitvoeren."

Hij koos voor de Motiv PST vanwege de laagdrempeligheid, gecombineerd met de goede naam die Motiv heeft in de markt. "Hoewel we nog geen klant waren bij Motiv, wisten we wel dat ze goed bekend staan in de markt. Ik vond het persoonlijk heel belangrijk dat zo'n test wordt uitgevoerd door een onafhankelijke partij. Ik zie het als een audit. Wij laten onze monteurs ook jaarlijks auditen door een onafhankelijk bedrijf, waarom zou ik dat niet op precies dezelfde manier aanpakken met security? Ons bedrijf is continu in ontwikkeling, de dreigingen ook. Het is goed om

jezelf met regelmaat door een onafhankelijke externe partij te laten doorlichten. Wij zijn daarom van plan om de PST periodiek, bijvoorbeeld jaarlijks, te laten doen."

Rapport in managementtaal
Motiv komt voor de PST een dag langs op de locatie van de klant. De dag start met een korte bespreking over de verwachtingen van de klant en eventuele vragen vooraf. Daarna zet de consultant een aantal vulnerability scans aan die interne systemen scannen op kwetsbaarheden. Voorafgaand zijn al enkele externe scans uitgevoerd. Daarna vinden er interviews plaats met de bij security betrokken IT-medewerkers. In die gesprekken komt alles aan bod, van netwerkbeveiliging tot awareness en van access management tot de kans op datalekken. De interviews duren maximaal een halve dag. Op die manier is er tijd over voor een snelle analyse van de belangrijkste kwetsbaarheden, zodat die eventueel direct kunnen worden aangepakt. De dag wordt afgesloten met een toelichting op de belangrijkste bevindingen. Een week later volgt een volledig rapport met een helder overzicht van aandachtspunten.

Starrenburg: "Ik was positief verrast door het rapport. Het is in managementtaal geschreven, met een heldere vertaalslag naar de techniek. Dat maakt het voor mij heel makkelijk om de resultaten met de rest van het managementteam te bespreken. Die missen immers de IT-achtergrond die ik wel heb. Het rapport beschrijft heel duidelijk waar de kwetsbaarheden zitten en welke impact die kunnen hebben. Door gebruik van de kleuren rood, oranje en groen weet je waar je het eerst mee aan de slag moet."

Aandacht voor techniek, mens en proces
Starrenburg was eveneens verrast door de compleetheid van het rapport. "Het belicht alles: technologie, processen, gedrag, awareness. Het is dus veel meer dan alleen een technische review."

Hoewel hij dacht dat hij een redelijk helder beeld had van de securitystatus, werd hij door sommige uitkomsten toch verrast. "Zo bleek er één applicatie die we weinig gebruiken verkeerd te zijn gepatcht. Daar waren we anders nooit achter gekomen. Ook in een extern systeem was een kwetsbaarheid gevonden, dat was echt wel een rode vlag."

Daarnaast is hij zich vooral nog meer bewust geworden van punten die hij eigenlijk wel wist. "Zo kregen we de aanbeveling om te gaan werken met een wachtwoordenkluis voor medewerkers. Daarmee maken we het voor hen makkelijker om maandelijks hun wachtwoord te wijzigen en een sterk wachtwoord te kiezen, zonder dat ik als eerstelijns support om de haverklap de vraag krijg om een wachtwoord te resetten omdat een medewerker het vergeten is."

Ook op het gebied van processen gaat 4Some nu dingen anders inrichten. "We nemen bijvoorbeeld de scheiding van rollen opnieuw onder de loep."

Jaarlijkse audit om vinger aan de pols te houden
Starrenburg is nu bezig met het maken van een plan van aanpak, gebaseerd op de door de PST gevonden kwetsbaarheden. "Sommige dingen zijn organisatorisch van aard, die gaan we gewoon regelen. Aan andere hangt een kostenplaatje. Dat betekent dat het managementteam akkoord moet gaan met de investeringen."

Hij is blij dat hij de PST heeft laten uitvoeren. "Je denkt snel: ik ben niet zo interessant. Maar iedere ondernemer heeft iets te verdedigen. Wij hebben bijvoorbeeld wel eens buitenlandse interesse gehad voor ons ERP-pakket, maar wij willen het IP niet verkopen. Dan moeten we het natuurlijk niet makkelijk maken om te stelen. Maar een nog groter gevaar zijn willekeurige ransomware-aanvallen waarbij het de hackers alleen maar om het losgeld is te doen. Het is fijn dat we nu weten waar hackers die wat meer moeite willen doen, binnen kunnen komen. We kunnen nu gerichte maatregelen nemen. Hackers zitten namelijk ook niet stil, wij kunnen ons dat ook niet veroorloven."