Be S(ec)ure!

Oplossing voor het verhogen van de digitale weerbaarheid.

SNELLE DETECTIE VORMT DE SLEUTEL TOT SUCCES!

De afgelopen tijd kunnen we vrijwel dagelijks in de media lezen, dat een organisatie is gehackt of geraakt door een aanval met ransomware. Hopelijk maakt dat ons allemaal voldoende alert op de digitale risico's die we met z'n allen lopen in de huidige wereld. De klassieke preventieve en defensieve maatregelen als firewall-oplossingen en anti-virusoplossingen zijn weliswaar goed, maar allang niet meer afdoende om een organisatie te beschermen.

Een professionele aanval, zoals onlangs bij Managed IT als partner van bijna honderd notariskantoren, is praktisch niet af te slaan. Vaak is het betalen van losgeld de enige optie om verder te kunnen met de bedrijfsvoering. Wel kunnen we de schade, zowel de technische, financiële als imagoschade met inzet van de juiste detectie-middelen aanzienlijk beperken.

We stellen u graag voor aan één van onze oplossingen die met directe alerting de sense-of-urgency aantoont:

- Snel en direct detecteren van brute-force aanvallen op RDP-endpoints
- Snel signaleren van kwaadaardig in- en uitgaand, horizontaal en verticaal verkeer (malware & ransomware)
- Snelle detectie van openstaande poorten en onjuiste Firewall-settings
- Snelle signalering van 'Shadow-IT' op het netwerk
- Snel signaleren van afwijkingen in gebruik van bandbreedte en datatransport
- Snel en eenvoudig in te richten zonder complexe installaties en netwerkaanpassingen
- Eenvoudig dashboard dat snel inzicht geeft en automatisch alerts verstuurt
- Gemakkelijk te integreren in de door GGI Veilig voorgeschreven SOC- en SIEM-inrichting uit perceel 1

HET IT | Industrieweg 5, 2712 LA, Zoetermeer | +31 079 59 39 384 | w.vandijk@het-it.nl | www.het-it.nl

HET BELANG VAN SNELLE DETECTIE

Onze oplossing heeft in meerdere omgevingen al **binnen 48 uur** ransomware kunnen detecteren. Dit betekent dat back-ups nog niet geïnfecteerd kunnen raken, waardoor de schade van een cyberaanval tot het minimum beperkt kan blijven en de organisatie snel weer up en running kan zijn. Het belang van snelle detectie is inmiddels ook door het Nationaal Cyber Security Centrum erkend en als basismaatregel opgenomen.

NATIONAAL CYBERSECURITYBEELD 2020:

"SNELLE DETECTIE KAN GEVOLGEN BEPERKEN, MAAR OVER HET ALGEMEEN DUURT HET LANG. HET VROEGTIJDIG DETECTEREN VAN AANVALLEN IS EEN BASISMAATREGEL. DES TE EERDER, DES TE BETER. DAT BLIJFT ECHTER VOOR VEEL ORGANISATIES EEN COMPLEXE OPGAVE."

"Volgens een onderzoek was in 2019 de gemiddelde detectietijd van een aanval 56 dagen. Deze gemiddelde detectietijd is niet in verhouding met de snelheid waarmee een aanvaller zijn doel kan bereiken. Die heeft slechts enkele uren nodig. In het jaarbeeld staat dat actoren snel misbruik maken van gepubliceerde kwetsbaarheden. Ook wanneer de aanvaller op minder snel succes uit is, bijvoorbeeld voor spionage, kan snelle detectie de schade beperken."

Deze alarmering neemt een steeds prominentere rol in, gelijk aan een brandalarm en een inbraakalarm. Diverse organisaties als **Innolux**, **Basic-Fit**, **Grolsch**, **Lucardi**, **Skyteam Airline Alliance Management Cooperatie**, **BK Ingenieurs** en **Trust Krediet Beheer** zijn inmiddels al aan de slag gegaan met deze detectie-oplossing, omdat de reeds aanwezige preventieve maatregelen niet meer voldoende bescherming bieden. Onze vendor-onafhankelijke last line of defence geeft real-time inzicht in alle verdachte verkeersbewegingen in het netwerk, en met name van alle datastromen van binnen naar buiten.

WAT WIJ DOEN

Wij bieden u de mogelijkheid van een Proof of Concept. Wij installeren op basis van de gebruikte bandbreedte een appliance in uw netwerk, die gedurende 4 weken al het netwerkverkeer zal monitoren en loggen. We analyseren samen de logbestanden, alerts en de getraceerde afwijkingen. We stellen vast welke kwetsbaarheden er zijn en bekijken in hoeverre ze een risico vormen voor de organisatie. Op deze wijze kunnen we snel achterhalen of en waar er door cybercriminelen aan de deur wordt gerammeld, tot op het niveau van de individuele werkplek.

Laat uzelf verrassen door de snelheid en eenvoud waarmee onze oplossing uw netwerk nog inzichtelijker maakt en ontdek in- en uitgaande datastromen die tot voor kort onzichtbaar waren voor uw organisatie. Zo kunnen wij al in een heel vroeg stadium slim de voorbereide ransomware-aanvallen detecteren en schade aan uw organisatie voorkomen.

HEEFT U INTERESSE?

Wij nodigen u graag uit om onze oplossing en aanpak nader toe te lichten.

H&T het it bv
hardware en technologie