Factsheet

identificatie als eerste stap naar een veiliger IT-infrastructuur

Ken de kwetsbaarheden van uw IT-omgeving voor een hacker ze vindt.

Moderne organisaties zijn steeds afhankelijker van een betrouwbare beveiliging van hun gegevens en systemen. Schijnbaar kleine risico's kunnen grote impact hebben als niet de juiste controlemechanismen worden toegepast. Weet u welke delen van uw organisatie en IT-infrastructuur kwetsbaar zijn voor indringers? Identificatie van deze zwakke plekken is de eerste stap op weg naar herstellende maatregelen voor een veilige en betrouwbare omgeving. Een grondige analyse van de kwetsbaarheden van uw organisatie en IT-omgeving is essentieel om de continuïteit van uw bedrijf te waarborgen.

De uitdaging

Alle onderdelen van uw IT-infrastructuur kunnen een bedreiging bevatten voor de bedrijfsprocessen die ze ondersteunen en daarmee voor het functioneren van uw organisatie. Elk systeem heeft zwakke plekken waarvan kwaadwillenden gebruik kunnen maken. Indringers verschaffen zich toegang tot uw netwerk via kwetsbare apparatuur of code en kunnen zelfs malware achterlaten.

Softwareproducenten balanceren voortdurend tussen gebruikersgemak en beveiliging van hun producten. Security heeft daarbij niet altijd de hoogste prioriteit. Standaard wachtwoorden zijn gevaarlijk. Wist u dat de softwarecode van een toepassing per definitie niet foutloos is? Elke 1000 regels code bevatten minstens zes bugs. Dit zijn zwakke plekken die hackers feilloos weten te vinden. Door proactief de kwetsbaarheden in uw IT-infrastructuur te reduceren, vermindert u de kans en impact van externe aanvallen met maar liefst 90%.

Onze oplossing

De Vulnerability Management Services (VMS) van Atos helpen u om het risico dat uw organisatie gehackt wordt te verkleinen. We gebruiken een combinatie van technologie, processen en jarenlange ervaring met het beveiligen van IT-systemen om uw infrastructuur en waardevolle data te beschermen tegen diefstal, verlies en schade.

Vulnerability Management kent drie pijlers:

- het periodiek scannen en testen van de securitystatus van de IT-infrastructuur;
- het bepalen van de compliancy van het security beleid;
- het oplossen van kwetsbaarheden in applicaties en systemen binnen de gescande infrastructuur.

VMS koppelt een architectuur met meerdere beschermingslagen aan een proactieve bestrijding van zwakke plekken. Kwetsbaarheden in de IT-infrastructuur worden hierdoor in een vroeg stadium opgespoord en hersteld. Als iemand met kwade bedoelingen toch toegang tot het bedrijfsnetwerk krijgt, is de kans minimaal dat deze schade kan aanrichten.

Identificatie als eerste stap naar een veiliger IT-infrastructuur

Atos past een 'state of the art' scanmethodiek toe en kan deze zowel eenmalig als periodiek uitvoeren. De rapportage is gerangschikt op prioriteit en business impact. Voor elke gevonden zwakke plek wordt aangegeven met welke actie deze geëlimineerd kan worden. Herstelacties kunnen hiermee gericht worden uitgevoerd op basis van uw prioriteiten.

Onze aanpak

De scope van de generieke scan stellen we samen met u vast en wordt uitgevoerd op een van tevoren vastgestelde interne of externe IP-reeks. De scan kan ook specifiek worden ingezet voor webapplicaties middels de door Atos ontwikkelde Internet Device Profiler. Deze specifieke scanmethode maakt gebruik van de Open Web Application Security Project (OWASP) methode en detecteert onder meer:

- zwakheden in cross-site scripting;
- gebreken van webpagina-implementaties;
- defecten van SQL Injection;
- onvolkomenheden in de webapplicatie-infrastructuur.
- backdoors.

Het dagelijks werk van uw organisatie wordt hier niet door beïnvloed. We analyseren, onderzoeken en documenteren de gevonden zwakheden en wij houden hierbij rekening met de risico's voor uw organisatie en uw IT-omgeving. U ontvangt een rapportage en een toelichting van onze Business Technologists. We doen aanbevelingen om de risico's te beperken en stellen samen met u vast of en welke verbeteracties noodzakelijk zijn. Daarna maken we een plan om de kwetsbaarheden op te lossen.

De voordelen

VMS is een toegevoegde waarde op de know-how en capaciteit van uw eigen organisatie. De dienst is ontworpen om beveiligingsrisico's inzichtelijk te maken, zodat deze gemitigeerd kunnen worden. Wij helpen u om de beveiliging van uw infrastructuur naar een hoger niveau te brengen.

Uw IT-infrastructuur is de basis van uw bedrijfsprocessen. Daarom is het belangrijk om regelmatig uw IT-infrastructuur te onderzoeken op kwetsbaarheden

Atos:

- scant elke twee weken vanuit Nederland meer dan 30.000 IP-adressen wereldwijd met behulp van 37 scanning tools;
- maakt het mogelijk om op veilige wijze zaken te doen via Internet;
- beschermt proactief de data van u en uw relaties en de koppelingen met de buitenwereld.

Extra services

Penetratietest & Ethical Hacking

Als aanvulling kunnen onze Business Technologists gebruik maken van tools om de kwetsbaarheden als test te exploiteren zoals kwaadwillenden dat ook zouden kunnen doen. Atos gebruikt dezelfde tools die een hacker zou gebruiken om kwetsbaarheden boven water te krijgen, waaronder NMAP, Nessus en Metasploit. We testen indringend alle bekende en onbekende systemen en diensten die verbonden zijn met uw netwerk en we produceren scripts voor het penetreren van uw IT-omgeving.

PCI-DSS Compliance scan

Organisaties die te maken hebben met creditcardbetalingen moeten voldoen aan de Payment Card Industry – Data Security Standard (PCI-DSS compliancy). Deze standaard vereist dat u elk kwartaal een gecertificeerde PCI-DSS compliance scan op uw IT-infrastructuur laat verrichten. Wij voeren deze scan voor u uit en leveren de rapportage.

Onze aanbieding

Atos laat u graag kennismaken met Vulnerability Management Services. Daarom bieden we u een standaard eenmalige Vulnerability Scan aan. Deze scan test kan op twee manieren worden uitgevoerd:

1. Een interne scan op een vooraf aangegeven lokale IP-reeks. Deze test wordt bij u op locatie uitgevoerd door onder meer een monitorkastje lokaal op uw netwerk aan te sluiten. Dit kastje heeft middels een firewallverbinding connectie met ons controlesysteem;
2. Een externe scan op een aantal IP-adressen dat vanaf het openbare internet bereikbaar is. Deze scan wordt op afstand uitgevoerd.

Onze Business Technologists bereiden samen met u de scan voor en na afloop van de scan ontvangt u een rapportage. Als uit de scan geen kwetsbaarheden blijken, dan is de test voor u gratis.

Uw IT-infrastructuur is de basis van uw bedrijfsprocessen. Daarom is het belangrijk om regelmatig uw IT-infrastructuur te onderzoeken op kwetsbaarheden. Wij helpen u graag met onze Vulnerability Management Services

Meer informatie

Atos
Papendorpseweg 93
3528 BJ Utrecht
+31 (0) 88 265 5555
nl.atos.net

Jaap Pinkster
Business Manager Security Services
jaap.pinkster@atos.net

Madlin dos Santos
Security Expert
madlin.dossantos@atos.net

securityNL@atos.net