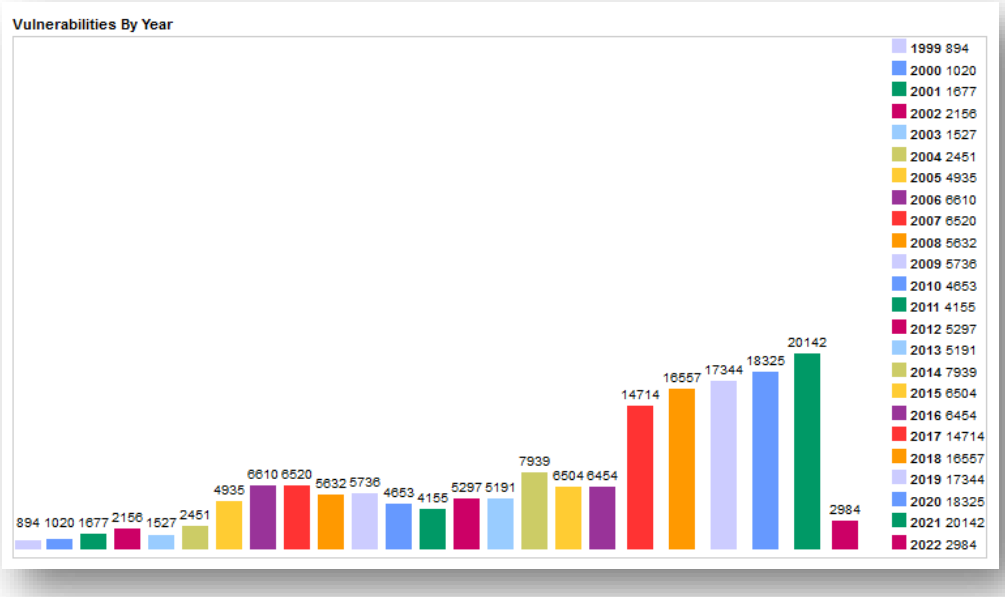
Optimale preventie met professioneel vulnerability *management*

Inleiding

Vulnerability management (managen van kwetsbaarheden) helpt bij identificatie, bescherming en detectie van kwetsbaarheden, malware en foutieve configuratie in uw systemen. In dit voorstel is beschreven waarom dit onderdeel van essentieel belang is en (veel) verder gaat dan alleen het zorgen voor patching en updating van systemen of het periodiek uitvoeren van een pentest of vulnerability assessment. In onze optiek is vulnerability management namelijk een noodzakelijk onderdeel om **'in-control'** te zijn of te komen op het gebied van informatiebeveiliging.

Toename in aantal kwetsbaarheden

Jaarlijks worden steeds meer kwetsbaarheden in hard- en software gevonden. Inmiddels zijn er meer dan 170.000 kwetsbaarheden bekend in hard- en software en worden onder andere bijgehouden in de Common Vulnerability and Exposures (CVE) database. Alleen in 2021 al zijn er 20.142 nieuwe kwetsbaarheden gevonden, waarbij de een meer uitgebreid in het nieuws komt dan de ander. Uw IT afdeling, eventuele security afdeling en/of extern IT leverancier(s) hebben wel de taak om alles bij te houden en zo snel als mogelijk te reageren op het moment dat zich een kwetsbaarheid voordoet. Maar hoe houdt u zicht of dit wel (tijdig) gebeurt? Nog steeds blijkt dat de helft van de aanvallen voorkomen had kunnen worden, doordat een kwetsbaarheid is misbruikt die al meer dan een jaar aanwezig is. Maar liefst 60% van de inbraken vindt plaats ondanks dat een patch beschikbaar was (maar blijkbaar niet is toegepast).



Bron: CVE-details.com, februari 2022

IT landschap dat continu wijzigt

Veel organisaties hebben een IT landschap dat continu in beweging is. Afgelopen periode zijn we massaal mobiel en thuis gaan werken. Cloud applicaties worden meer en meer ingezet en steeds vaker maken we gebruik van Infrastructure as a Service. Daarnaast wordt Internet of Things (IoT) steeds meer toegepast. Hoe houdt u zicht en controle op (de kwetsbaarheid van) deze systemen en applicaties? Veel organisaties hebben geen continu zicht op wat er allemaal aan het netwerk wordt aangesloten en of die apparatuur en software wel veilig is.

Prioriteiten stellen en budgetbewaking

Doordat het landschap wijzigt en er zo enorm veel kwetsbaarheden zijn waar aandacht aan gegeven moet worden, wordt het steeds belangrijker om de juiste prioriteiten te stellen. Eigenlijk wilt u dat uw security team of IT afdeling zich bezighoudt met de risico's die écht belangrijk zijn. Dit hoeven niet altijd de systemen met kwetsbaarheden te zijn met een hoge CVSS score[1]. CVSS houdt namelijk geen rekening met het feit of de kwetsbaarheid ook werkelijk wordt misbruikt. Daarnaast houdt CVSS ook geen rekening met het systeem waarop de kwetsbaarheid zich voordoet, waardoor een kwetsbaarheid op een laptop dezelfde prioriteit krijgt toegewezen als eenzelfde kwetsbaarheid die zich voordoet in een belangrijk ERP systeem met alle klantdata. Dit alles betekent dat een IT afdeling bezig kan zijn met totaal verkeerde werkzaamheden en juist de kwetsbaarheden mist die er toe doen. In feite wilt u zich vooral richten op kwetsbaarheden waarbij de kans op misbruik hoog is en het systeem waarop (of de context waarin) de kwetsbaarheid zich voordoet van groot belang is voor uw organisatie. In feite bepaalt de combinatie hiervan het werkelijke risico voor uw organisatie.

Een voorbeeld hierbij is de recente log4J kwetsbaarheid. Log4J is een hulpprogramma voor logging in applicaties, dat bijvoorbeeld ook in de veelgebruikte webserver software van Apache wordt gebruikt. In december 2021 is een zogenaamde zero-day kwetsbaarheid geconstateerd in deze software, wat wil zeggen dat er op moment van constateren en naar buiten brengen nog geen patch voorhanden was. Dit betekent over het algemeen een groot risico op misbruik. Wij zien dat veel organisaties dagen, zo niet weken zijn bezig geweest om in kaart te brengen waar de Log4J kwetsbaarheid zich voor zou kunnen doen om vervolgens risico beperkende of mitigerende maatregelen uit te voeren. Veel organisaties hadden hierbij niet de juiste afstemming met hun leveranciers. Dat veel organisaties in deze periode een verhoogd risico hebben gelopen (of nog steeds lopen) mag duidelijk zijn. Eigenlijk wil je met één oogopslag direct zien welke systemen kwetsbaar zijn en waar actie moet worden ondernomen.

Regelgeving, compliancy, audits, SLA's en rapportages

De druk van regelgeving en rapportage neemt toe. Zowel interne stakeholders (bestuur, directie en management) als externe stakeholders (accountants, verzekeraars, wetgever etc.) willen aantoonbaar weten hoe processen rond informatiebeveiliging zijn geborgd. Daarnaast wordt de ketenwerking steeds belangrijker. (Grotere) klanten zullen steeds vaker gaan vragen hoe u zorgt voor continuïteit in uw systemen en vertrouwelijkheid/integriteit van uw informatiestromen. Stilvallen of inbreuken in úw processen of informatie kan ernstig nadelige gevolgen hebben voor uw klanten. Kortom, meten en aantonen wordt steeds belangrijker.

In dit kader betekent e.e.a. dat u ook weer moet weten hoe de partijen waar u diensten van afneemt hun informatiebeveiliging hebben verzorgd. Hiervoor worden over het algemeen Service Level Agreements (SLA's) afgesloten, maar hoe weet u dat uw leverancier of IT afdeling doet wat is belooft? Hoe bewaakt u deze SLA's continu op basis van werkelijke data in plaats van op basis van een ingevulde vragenlijst of informatie die wordt aangeleverd? Juist hier werken wij in de driehoeksverhouding tussen u (opdrachtgever), IT leverancier of IT afdeling en ThreadStone. Onafhankelijk en transparant geven wij aan waar wij kwetsbaarheden binnen uw organisatie zien.

[1] Common Vulnerability Scoring System bepaalt de criticaliteit van een kwetsbaarheid op basis van een theoretische score

Vulnerability management van ThreadStone

Als u geen eigen security afdeling heeft of als uw security afdeling beperkt tijd heeft, dan adviseren we om vulnerability management uit te besteden. In dat geval zorgen wij – naast inrichting en configuratie - voor de inhoudelijke controle op kwetsbaarheden en het afstemmen hiervan in de driehoeksverhouding tussen u, IT verantwoordelijke en ThreadStone. Zo werken we gezamenlijk naar continue verbetering en preventief veilig houden van uw systemen en software. U kunt daarbij het volgende van ons verwachten:

- We helpen uw organisatie met implementatie van risicogebaseerde Vulnerability management op basis van machine learning. Geen eenmalige scans of scans die bijvoorbeeld 1x per jaar worden uitgevoerd, maar continu scannen en monitoren van de omgeving;
- We zorgen voor ondersteuning bij de eerste implementatie en configuratie van vulnerability management. Denk hierbij aan (ondersteuning bij) installatie van scanners, agents, configuratie van gebruikersbeheer, dashboards, credentials en reporting die we opzetten;
- We controleren uw systemen continu op kwetsbaarheden en fouten in configuraties en zorgen voor afstemming met uw (externe) IT afdeling om e.e.a. te mitigeren. Daarbij richten we ons op kwetsbaarheden die werkelijk van belang zijn voor uw organisatie;
- We zorgen dat uw IT specialisten kunnen werken met de tooling. Zij leren daarmee risico's zo snel mogelijk te onderkennen en zo min mogelijk tijd te verspillen met onderzoeken van kwetsbaarheden die niet relevant zijn;
- Externe leveranciers krijgen een eigen inlog waarmee ze de kwetsbaarheden van het deel waar zij verantwoordelijk voor zijn realtime kunnen inzien. U komt hiermee in de positie om SLA beheer naar een hoger niveau te tillen;
- We melden direct op het moment dat er een kwetsbaarheid wordt gedetecteerd die aan bepaalde kwalificaties voldoet (volgens best practices en afhankelijk van de snelheid dat onze scanners de kwetsbaarheden kunnen detecteren);
- We spreken periodiek de situatie door en bepalen in overleg welke acties moeten worden uitgevoerd;
- We rapporteren periodiek op geconstateerde kwetsbaarheden, opgeloste kwetsbaarheden en eventueel behalen van overeengekomen SLA's met uw leveranciers;
- We rapporteren periodiek op nieuwe apparaten;
- We rapporteren indien credentials niet (meer) werken;
- We rapporteren periodiek op compliancy t.b.v. hoger management;
- We leveren support op de omgeving (8x5).

Uitgangspunten

Bij ons vulnerability management gelden een aantal uitgangspunten:

- Wij houden contact met een vaste contactpersoon bij uw organisatie. Bij de verschillende overleggen is het uiteraard om meerdere personen – ook van leveranciers – uit te nodigen, maar de initiatie hiervan ligt bij u;
- Wij leveren scanners die geplaats kunnen worden in het netwerk (in overleg virtueel of hardware units). Uw IT specialist dient te zorgen voor de installatie van deze scanner. In overleg kunnen we meerdere scanners leveren die in verschillende segmenten worden geplaatst;
- Wij leveren agents (stukje software) die geïnstalleerd kunnen worden op laptops en thuiswerkplekken. Uw IT specialist dient te zorgen voor de installatie van deze agents;
- U of uw IT specialist zorgt voor invoer en bijhouden van credentials. Wij zorgen voor het beschikbaar stellen van accounts waarmee de credentials kunnen worden ingevoerd of gewijzigd, wij zullen in onze dienstverlening dus geen credentials invoeren of onder ogen krijgen;

Optionele diensten

Over het algemeen starten we met inrichting van bovenstaande vulnerability management. Hiernaast is het mogelijk om extra diensten af te nemen, zoals:

- Geavanceerde web application scanning die wordt opgenomen binnen het vulnerability management, eventueel aangevuld met PCI ASV controles (t.b.v. creditcards);
- Active directory scanning wordt opgenomen binnen het vulnerability management;
- Het controleren van OT/Scada systemen wordt opgenomen binnen het vulnerability management;
- Container security voor devops wordt opgenomen binnen het vulnerability management;
- Er worden meer uitgebreide vormen van dashboards, alerting, reporting of integraties met andere systemen opgezet.

Waarom ThreadStone

- We leveren security-advies (beleid/organisatie, mens en techniek), met name voor organisaties zonder eigen security afdeling;
- We helpen om de weerbaarheid van uw organisatie (blijvend) te verbeteren en verhogen uw security 'volwassenheidsniveau'. Hier worden verschillende diensten voor ingezet, afhankelijk van het huidige niveau van security, uw wensen en uw budget;
- Ons doel is om gezamenlijk – met onder andere (extern) IT beheerder(s) – te komen tot verbetering. Hiervoor houden we een spiegel voor en geven we onafhankelijk advies over de maatregelen die uw organisatie kan nemen om risico's te beperken;
- ThreadStone is een Nederlandse onderneming, met korte lijnen en kennis en ervaring in de Nederlandse markt.