Vulnerability Scanning

Voorkom onnodige risico's in uw datacenter en patch op tijd

Het is vaak als nieuws over beveiligingslekken de media halen dat organisaties zich pas bewust worden van het risico dat ze lopen. Wist u dat het **niet-patchen van software vandaag één van de top drie toegangswegen voor hackers is**? De meerderheid van succesvolle cyberaanvallen is immers terug te voeren op een bekende kwetsbaarheid die niet werd aangepakt. Of erger nog: op een kwetsbaarheid die de organisatie helemaal niet kende.

In 2022 werd er wereldwijd een recordaantal van 26.448 beveiligingslekken in software gemeld. Het aantal kritieke kwetsbaarheden nam ten opzichte van 2021 met 59% toe tot 4.135. Alleen al het continu in kaart brengen van al die nieuwe kwetsbaarheden is een hele opdracht. In combinatie met de beperkte middelen waarover IT-teams beschikken, leidt dat al gauw tot **inefficiëntie**. Maar wat veel erger is: het resulteert ook in **een nodeloze blootstelling aan perfect vermijdbare risico's**.

Dankzij onze **Vulnerability Scanning** hoeft het opsporen van kwetsbaarheden niet per definitie een dure en tijdrovende bezigheid te zijn. Onze oplossing helpt uw IT-medewerkers bij het identificeren en analyseren van enorme hoeveelheden bekende kwetsbaarheden. De tijd die zo vrijkomt, kunnen zij voortaan nuttiger besteden. Aan het tijdig patchen van al die kwetsbaarheden, bijvoorbeeld. Zo verlegt u de **focus** van het opsporen **naar het effectief oplossen van uw beveiligingsproblemen**.

inetum realdolmen
Positive digital flow

Vulnerability Scanning: security voor een vaste prijs

Het aantal apparaten dat u wil scannen op kwetsbaarheden bepaalt het budget van onze dienstverlening. Ons basispakket voor Vulnerability Scanning omvat een eerste reeks van 500 apparaten. Dat starterspakket kan u aanvullen met extra pakketten van telkens 250 apparaten. Zowel voor het basispakket als voor de aanvullende pakketten geniet u een vast tarief. Zo weet u steeds waar u financieel aan toe bent en komt u achteraf niet voor onaangename verrassingen te staan.

Onze aanpak: voorkom onnodige risico's in 5 stappen.

1. **Kick-off met intakegesprek**: Een eerste gesprek helpt ons uw wensen te begrijpen en het precieze aantal apparaten te bepalen die we voor u op kwetsbaarheden moeten scannen. Op basis van die voorbereidende analyse selecteert u vervolgens het pakket dat het meest voor u geschikt is.
2. **Klantbezoek met implementatie**: Wij komen onze oplossing voor Vulnerability Scanning op een toestel die we zelf voorzien bij u ter plaatse installeren en correct configureren, helemaal op uw maat. Wij doen dat in grondig overleg en nauwe samenwerking met uw eigen IT-verantwoordelijken.
3. **Gegevensverzameling**: Onze oplossing verzamelt gegevens over uw apparaten, inclusief informatie over kwetsbaarheden, verkeerde configuraties en andere beveiligingsproblemen.
4. **Analyse op afstand**: Wij verwerken en analyseren de data in ons analysecentrum. Die analyse identificeert beveiligingsproblemen en kent aan elk probleem een risicoscore toe.
5. **Rapportering**: Wij bezorgen u een rapport met een samenvatting van de geïdentificeerde beveiligingsproblemen, hun risicoscores en de maatregelen voor herstel die wij prioritair aanbevelen. Zo helpt ons rapport u om de meest kritieke beveiligingsproblemen als eerste aan te pakken.

Onze Vulnerability Scanning zit erop. Wat nu?

Enkel een **proactieve benadering** van cybersecurity kan u op uw beveiligingsuitdagingen een passend antwoord bieden. Anders gezegd: kwetsbaarheden in uw datacenter moet u opsporen en aanpakken vóór criminelen ze kunnen uitbuiten.

Dat lijkt evident, maar de harde waarheid is helaas dat u altijd kwetsbaarder bent dan u denkt. Daarom is het belangrijk om alle mogelijke **kwetsbaarheden via regelmatige scans te identificeren**. Die **Vulnerability Scanning** is de noodzakelijke eerste stap in een veel ruimer proces van **Vulnerability Management**. Dat proces omvat verder ook nog:

- een grondige **beoordeling** van de risico's die aan elke kwetsbaarheid zijn verbonden
- een **prioritering** van de geïdentificeerde kwetsbaarheden
- de opstelling van een plan om alle kwetsbaarheden tijdig te **verhelpen**

Inetum-Realdolmen heeft alle nodige expertise in huis om u doorheen die verschillende stappen deskundig te adviseren en technologisch te ondersteunen.

Meer info?

Bij onze experts kan u steeds terecht met al uw vragen en verzoeken, ideeën en suggesties.
Zij informeren u graag ook over andere diensten die Inetum-Realdolmen kan bieden:

info@inetum-realdolmen.world