fit secure
ICT & SECURITY EXPERTS

- Cloud
- Security
- ICT Sanity
- ICT Managed Services

Vulnerability Management

Preventief scannen van (on)beheerde apparatuur als nieuwe standaard

Cyberdreigingen ontwikkelen zich razendsnel. Updates en patches zijn belangrijk, maar niet voldoende: je moet weten waar de kwetsbaarheden zich bevinden, óók buiten de systemen die je beheert. Met onze dienst Vulnerability Management krijg je continu inzicht in risico's binnen je volledige netwerk, beheerd én onbeheerd, zodat je sneller kunt ingrijpen en voldoen aan moderne beveiligingsrichtlijnen zoals NIS2.

Continu scannen op kwetsbaarheden

Wij voeren 24/7 geautomatiseerde kwetsbaarheidsscans uit op:

- Beheerde werkplekken, servers en netwerkapparatuur
- Onbeheerde apparaten zoals printer, IoT-apparaten, mobiele telefoons
- (Gast)netwerken, kantooromgeving en apparaten die tijdelijk of incidenteel verbinden
- Intern én extern gehoste applicaties en servers
- Websites en webapplicaties van jouw organisatie

Van inrichten naar continu bewaken

Onze aanpak sluit naadloos aan op onze visie:

- Niet alleen inrichten, maar ook continu bewaken
- Altijd afgestemd op de laatste richtlijnen
- Inzicht, controle en zekerheid over je volledige netwerk

Deze continue monitoring zorgt voor een 360-graden beeld van alle risico's in jouw IT-omgeving.

fit secure
ICT & SECURITY EXPERTS

- Cloud
- Security
- ICT Sanity
- ICT Managed Services

Vulnerability Management

Preventief scannen van (on)beheerde apparatuur als nieuwe standaard

Waarom Vulnerability Management

1. Inzicht in alle risico's binnen je netwerk

Je ziet precies welke kwetsbaarheden aanwezig zijn, wat de impact is en waar prioriteit moet liggen. Dit vormt de eerste en belangrijkste stap van risicobeheersing binnen NIS2.

2. Uitgebreide rapportage en risicoanalyse

We leveren heldere rapportages die direct inzicht geven in het aantal en type kwetsbaarheden, de risicoclassificatie, aanbevelingen voor opvolging en relevante trends binnen jouw organisatie. De rapportages worden automatisch gefilterd op urgentie, type kwetsbaarheid en impact, zodat je in één oogopslag ziet waar actie nodig is.

3. Extra controle voor beheerde apparaten

Voor systemen die wij al beheren voeren we een extra diepgaande kwetsbaarheidscontrole uit. Hiermee toetsen we onze eigen patching en krijgen we inzicht in risico's afkomstig van niet-standaard of zelf geïnstalleerde software.

Wij zijn jouw partner in cybersecurity. Veilig werken, daar gaan we voor, daar staan we voor.