DNA
Business first.

dnaservices.nl

Security scan

Inleiding

DNA biedt bedrijven een security scan aan waarmee de volledige infrastructuur kan worden gecheckt op kwetsbaarheden en configuratieproblemen.

Naast een interne check van de systemen wordt er ook gecheckt op eventuele kwetsbaarheden en bedreigingen van buitenaf. Zo kunnen wij een goed beeld geven van uw huidige situatie.

Want zoals u wellicht weet, is tegenwoordig het adagium: 'it's not the question *if* you will be hacked, but *when* you will be hacked!'

Een veel voorkomend voorbeeld van een mogelijk beveiligingslek is het onvoldoende toepassen van patchmanagement. Hierdoor kunnen personen en bedrijven met minder goede bedoelingen uw bedrijf elektronisch binnendringen. Dit doen ze bijvoorbeeld door malware te installeren en vervolgens bedrijfs-gevoelige data te ontvreemden.

Nadat wij bij uw organisatie een security scan hebben uitgevoerd ontvangt u een rapportage met daarbij een advies.

Security scan

- Kwetsbaarheden detectie
- Netwerkscan
- Rapportage
- Voorkomen van hacks

Betrouwbaar, veilig en snel werken in de Cloud

DNA Services B.V.
Sandelingenstraat 38b
3342 BM Hendrik-Ido-Ambacht
+31 (0) 78 65 45 777
info@dnaservices.nl
www.dnaservices.nl

Bent u benieuwd wat DNA voor u kan betekenen?
Neem dan contact met ons op.

Netwerkdetectie

De security scan controleert het complete netwerk waaronder werkplekken, routers, switches, (next generation) firewalls, SAN, NAS, servers, OS (Windows, Linux, etc.), webservers, netwerkprotocollen, certificaten, VPN-verbindingen, encryptieprotocollen en gevoelige data. Vrijwel alle componenten en kritische infrastructuur die in een netwerk aanwezig zijn plus de daarbij behorende datacommunicatie (poort scan) gecheckt. Onze tooling voor deze scan is bijgewerkt met de meest recent vrijgegeven patches, ontdekte kwetsbaarheden en malwaredetectie.

Rapportage

Naar aanleiding van de security scan ontvangt u een uitgebreid rapport over de status van uw netwerk, de eventueel aangetroffen gevoeligheden én een advies hoe u deze kwetsbaarheden kunt voorkomen of repareren. DNA beschikt daarnaast over expertise en tooling die u kunt inzetten om de meeste kwetsbaarheden structureel op te lossen en te monitoren.

Systeemvereisten

Om de security scan uit te voeren is een virtuele omgeving vereist waarop onze tooling geïnstalleerd kan worden. Indien deze niet beschikbaar is zorgen wij zelf voor een systeem om dit te installeren. Dit systeem wordt tijdens de security scan geplaatst in uw netwerk. In verband met de netwerkbelasting en performance is het advies om de scan indien mogelijk buiten reguliere werktijden uit te voeren.

Consequenties

Uiteindelijk blijft u als klant eindverantwoordelijk voor uw netwerk. Het doel van de security scan is daarom u bewust te maken van de huidige status van uw netwerk en door middel van een plan van aanpak uw netwerk continu up-to-date te houden om de kans op digitale inbraken zo klein mogelijk te maken. Want zoals u wellicht weet, is tegenwoordig het adagium: ‘it’s not the question *if* you will be hacked, but *when* you will be hacked!’

Advies

Gezien de technologische ontwikkelingen en de toename van digitale dreigingen, is ons advies een security scan periodiek uit te voeren (minstens 1 of 2 keer per jaar).

Meer informatie

Voor meer informatie kunt u contact met ons opnemen via onze website, per e-mail of via de telefoon.

DNA Services B.V.
Sandelingenstraat 38b
3342 BM Hendrik-Ido-Ambacht
+31 (0) 78 65 45 777
info@dnaservices.nl
www.dnaservices.nl