

Security Scan

De verbindingen van uw bedrijfsnetwerk met het internet zorgen voor sterk verhoogde beveiligingsrisico's. Met onze Security Scan kunnen wij de door u genomen beveiligingsmaatregelen verifiëren en de kwetsbaarheid van uw applicaties toetsen volgens de laatste inzichten.

Security Scan

Vanveen informatica heeft sinds 1987 een sterke reputatie opgebouwd in het beheer van netwerken en applicaties. Daardoor heeft Vanveen informatica veel kennis en ervaring in huis om u te helpen in het benoemen van de beveiligingsrisico's van uw netwerk.

Het doel van onze Security Scan is om de mate van kwetsbaarheid voor aanvallen via uw internetverbinding van alle door u gebruikte systemen en applicaties vast te stellen. Door aanvallen van hackers kunnen uw systemen en applicaties beschadigd worden, zodanig dat gebruik tijdelijk niet meer mogelijk is. Ook kunnen belangrijke bedrijfsgegevens op straat komen. Hackers bedienen zich daarbij van de laatste ontdekkingen op het gebied van softwarelekken (zgn. *exploits*). Hiervoor dienen bepaalde beveiligingsupdates van uw softwareleverancier te worden aangebracht.

Uw voordelen

Met de resultaten van dit onderzoek heeft u meer inzicht in de risico's die uw organisatie loopt en in de te nemen maatregelen die deze risico's verkleinen. U kunt op basis van ons onderzoek een weloverwogen beslissing nemen of deze maatregelen, al dan niet gedeeltelijk, moeten worden genomen.

De volgende producten zullen na afronding van de Security Scan worden opgeleverd:

- Rapport met conclusies en aanbevelingen, gebaseerd op de gevonden kwetsbaarheden en de daaraan gekoppelde risico's.
- Verklaring van vernietiging van alle verzamelde informatie.
- Evaluatiegesprek over geleverde product.

De conclusies en aanbevelingen die gedaan worden, kunt u, geheel of gedeeltelijk, door Vanveen informatica, laten uitvoeren.

Werkwijze Security Scan

De Security Scan moet inzicht opleveren in hoeverre uw systemen en applicaties kwetsbaar zijn voor aanvallen via uw internetverbinding.

Tijdens dit onderzoek worden de systemen en applicaties in uw netwerk geïnventariseerd en beoordeeld op hun kwetsbaarheid op basis van onze laatste informatie. Daarbij wordt gebruik gemaakt van de verschillende bronnen, zoals van bijvoorbeeld gevestigde organisaties op het gebied van netwerk- en applicatie-beveiliging, diverse waarschuwingdiensten, maar ook van uw softwareleverancier(s).

Vervolgens wordt met uw toestemming via uw internetverbinding een aantal testen uitgevoerd, waaruit een mogelijke kwetsbaarheid blijkt (ethical hack). Daarbij worden o.a. uw web- & mail-servers en firewall op kwetsbaarheden (zoals verouderde softwareversies, bekende beveiligingslekken e.d.) onderzocht. Hierbij zullen gangbare test-scripts worden gebruikt, maar ook minder bekende technieken. Alle werkzaamheden van deze fase zullen worden gelogd en worden opgenomen in de uiteindelijke rapportage.

Voor het uitvoeren van ons onderzoek zijn de volgende randvoorwaarden belangrijk:

- Technische en organisatorische informatie over de internettoegang en componenten.
- Schriftelijke vrijwaring en machtiging door u om de internettoegang aan diverse testen te onderwerpen.
- Een contactpersoon namens u die tijdens het onderzoek kan worden benaderd.

De voorbereidingen en werkzaamheden van deze dienst worden met een hoge mate van zorgvuldigheid verricht. Zo hanteert Vanveen informatica een strak protocol van oplevering, geheimhouding en vernietiging, waarmee wordt gewaarborgd dat uw vertrouwelijke gegevens zorgvuldig worden gebruikt.

Andere producten

Op uw verzoek kunnen wij de Security Scan combineren met onze Ethical Hack en Social Engineering producten. Met deze rapportages kan een zeer uitgebreid en compleet beeld worden verkregen van de beveiliging van uw ICT-infrastructuur.

Onze Security Scan kan ook worden gecombineerd met de Performance- en Availability Scan, zodat uw applicatie-systeem op alle belangrijke aspecten kan worden doorgelicht. Van deze producten zijn aparte beschrijvingen beschikbaar.

Onze benadering

Vanveen informatica gebruikt in haar aanpak de bekende PDCA-cirkel afkomstig uit het kwaliteitsdenken. PDCA staat voor Plan, Do, Check en Act, vier processtappen om te komen tot een continue verbetering van een product of proces. De eerste Plan-stap bestaat uit twee delen: vaststellen doel en vaststellen middelen. De tweede Do-stap bestaat uit het implementeren van het plan. In de derde Check-stap wordt het resultaat gemeten en gerapporteerd. In de vierde Act-stap wordt besloten welke veranderingen nodig zijn om het proces te verbeteren, waarna opnieuw de cyclus kan worden doorlopen.

Met onze Audit-, Review-, Analyse- en Scan-producten kunt u uw ICT-infrastructuur door ons laten controleren en adviseren over mogelijke verbeteringen (Check). Met onze rapportages kunt u een duidelijke keuze maken hoe verder te gaan (Act). Met onze kennis en ervaring kunnen wij u vervolgens behulpzaam zijn bij het opstellen van het projectplan (Plan) en de uitvoering ervan (Do).

Over Vanveen informatica

Als zelfstandige, onafhankelijke ICT kennisorganisatie, actief vanaf 1987, hebben wij een jarenlange ervaring in het beveiligen van de netwerken van de overheid en de internet-security van diverse financiële instellingen.

Wij kunnen u helpen bij het ontwikkelen, implementeren en onderhouden van een doordachte beveiliging, preventief, curatief en repressief: Incidenten voorkomen, er snel en slagvaardig op reageren en maatregelen nemen om gevolgschade te voorkomen. Daarbij kunnen wij u zowel adviserend als operationeel van dienst zijn en u aldus met raad en daad terzijde staan.

Meer informatie

Voor meer informatie kunt u contact opnemen met Rick Strijbos, telefoon 079-3430909 of per e-mail strijbos@vanveen.nl.

Kijk voor een compleet en actueel overzicht van onze producten op www.vanveen.nl.

