

Externe Security Audit

In een security audit worden diversen aspecten van de actuele situatie van de netwerkinfrastructuur grondig onderzocht op veiligheid. Met behulp van zowel interne- als externe security audits kan meer inzicht worden verkregen in de mate waarin data risico loopt gecompromitteerd te worden. Een security audit is aan te raden bij het bedenken, implementeren en upgraden van security maatregelen en nadat acties zijn ondernomen. Het doel van de analyse is inzicht verwerven in:

- Dreigingen ten aanzien van de IT infrastructuur
- De kans dat de dreigingen daadwerkelijk zullen plaatsvinden
- De kosten die een eventuele inbreuk kan veroorzaken

De security audits geven een goed beeld van de echte bedreigingen waar een onderneming of instelling mee te maken kan krijgen. Een security audit is dan ook essentieel om te kunnen bepalen welke acties ondernomen dienen te worden om de risico's te beperken .

De Externe Security Audit is een consultancydienst van Hemelaar Networking, waarbij een ervaren consultant alle actieve netwerkcomponenten zoals publiekelijk toegankelijke servers, firewalls en routers test. Door middel van scantools en handmatige testen en onderzoeken wordt een rapport gemaakt . Dit rapport geeft inzicht in de risico's die het netwerk loopt ten aanzien van de systemen die geaudit zijn. En is voorzien van aanbevelingen om deze risico's te minimaliseren. Tevens zal het rapport door de consultant worden toegelicht.

De technieken die gebruikt worden in onze scans variëren van de automatische scantool van Beyond Security tot handmatige datamanipulatie.

Het is de bedoeling om zo geen schade aan te richten en alleen te detecteren dat er schade aangericht kan worden, het is echter niet altijd te voorkomen dat een apparaat na een scan niet meer naar behoren functioneert. Het is daarom van belang dat vooraf back-up's van de target systemen te maken en tijdens de scan de systemen door de verantwoordelijke netwerkbeheerders gemonitord worden. Hierdoor kan er snel worden ingegrepen.

Tijdens de Externe Security Audit wordt er gekeken of er 'achterdeuren' aanwezig zijn in operating systemen of applicaties en of er risicovolle programmatuur en/of services actief zijn. Hierbij kan gedacht worden aan programma's die onbewust toegang verlenen aan hackers, of ongewenst informatie naar buiten sluisen.

Daarnaast worden alle systemen die onder de test vallen gecontroleerd op aanwezigheid van alle voorgeschreven patches en bugfixes. Tevens wordt er gecontroleerd op configuratiefouten die gevaarlijk zijn voor de systemen dus voor continuïteit van de ICT omgeving. Er wordt daarbij gebruik gemaakt van de meest gebruikte hackingmethodes voor de verschillende besturingssystemen en services.

De duur van de test is afhankelijk van het aantal IP adressen en systemen die onder de audit vallen. De processen vinden veelal parallel plaats waardoor de benodigde tijd voor een extra IP adres of systeem wordt beperkt.

Inhoud van de externe audit:

Stap 1: audit

- Publiek domein
- Firewall:
- Servers: (scanning van webservers, mailservers, FTP servers)
- Internet router(s)
- portscanning;
- OS detectie;
- SNMP detectie;
- Vulnerability tests

Stap 2: rapportage en advies

Kosten:

Prijzen per scan:	IP adressen	Prijzen
Éénmalige scan	1-5	€450,-
	5-10	€950,-
	>10	Op aanvraag
Scan abonnement 2x per jaar	1-5	€750,-
	11-50	€1.650,-
	>10	Op aanvraag

Opmerking:

Alle prijzen zijn excl. BTW, wijzigingen en drukfouten voorbehouden.