Sårbarhetsanalys

Sårbarhetsanalys är en säkerhetstjänst som löpande kontrollerar IT-system och rekommenderar åtgärder.

Tjänsten vänder sig i första hand till företag med system och applikationer som kommunicerar via Internet och därmed ständigt är utsatta för säkerhetshot. För företag med system som hanterar finansiella transaktioner, innehåller känslig data eller har externa säkerhetskrav är tjänsten extra värdefull.

Hur sårbara är dina IT-system?

Bristande säkerhet kan leda till att externa parter kommer åt känslig information eller får möjlighet att påverka IT-system. Internetbaserade system är ständigt utsatta för säkerhetshot i form av intrångsförsök eller andra typer av attacker. Ofta finns det även externa krav på hög säkerhet från kunder eller regelverk. Därför behövs löpande säkerhetskontroller som minimerar risken för sårbarheter. Tjänsten ger ett kvitto på att era system är konfigurerade på ett säkert sätt.

Sårbarhetsanalys

Funktioner och fördelar med sårbarhetsanalysen:

- Minskar risken för intrång och attacker.
- Baserad på marknadens mest använda system för sårbarhetsskanning.
- Kontrollerar över 60 000 olika sårbarheter och konfigurationer.
- Löpande tjänst som återkommande verifierar säkerheten i dina system.
- Färdig tjänst, ingen separat installation behövs.
- Tripnet hanterar all konfiguration.
- Rapport, analys och åtgärdsplan från Tripnet.

I kombination med Tripnets drifttjänster för infrastruktur, operativsystem och applikationer hjälper vi er att hålla programvaror uppdaterade och systemen säkert konfigurerade.

Kontinuerligt säkerhetsarbete

Sårbarhetsanalysen skannar av externa IP-adresser, servrar eller hela nät efter kända sårbarheter. Det ger er mycket god information om eventuella säkerhetsrisker samt vilka åtgärder som bör vidtas. Tjänsten är baserad på Nessus från Tenable, en av marknadens mest använda produkter för sårbarhetsskanning. Den kräver ingen infrastruktur eller installation.

Säkerhetsarbetet inleds med ett uppstartsmöte för att definiera omfattningen av analysen. Tripnet utför allt förberedande arbete med nät, brandväggar och konfiguration av skanningstjänsten. Efter genomförd skanning tar Tripnet fram och analyserar rapporter som överlämnas tillsammans med rekommendationer på eventuella åtgärder. Sårbarhetsanalysen utförs därefter kvartalsvis så att ni får löpande kontroll av systemen och fångar upp eventuella förändringar som kan påverka säkerheten.

Kompetens och proaktivitet

Tripnets sårbarhetsanalys är en färdig tjänst som inte kräver några resurser av er organisation. Serversystem och mjukvaror finns redan på plats och kan snabbt tas i bruk. Våra tekniker arbetar dagligen med säkerhetsfrågor och har lång erfarenhet av systemdrift. Det innebär att ni får bra analyser och möjlighet till snabb och professionell hjälp med eventuella åtgärder.

Tillsammans med våra drifttjänster får ni en komplett lösning för säker drift och kontroll av era IT-system. Genom proaktiva uppdateringar och löpande sårbarhetsanalyser med Nessus marknadsledande mjukvara får ni en mycket bra plattform för säkra och tillgängliga IT-system.

TRIPNET

Tjänster som ingår i Sårbarhetsanalys

Tjänst	Ingår	Tillval
Sårbarhetsskanning med Nessus Vulnerability Scanner	✓	
Kvartalsvis rapport och analys	✓	
Rapport och analys med annat intervall		●
Uppstartsmöte	✓	
Konfiguration av tjänsten	✓	
Skanning av definierade IP-adresser och servrar	✓	
Presentation av analys på plats hos Tripnet eller via telefon/webb	✓	
Extern skanning mot publikt åtkomliga adresser	✓	
Intern skanning på servrar	✓	
Nätverksenheter: Juniper, Cisco, Palo Alto, brandväggar etc.	✓	
Operativsystem: Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM iSeries	✓	
Databaser: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL	✓	
Webbapplikationer: OWASP Top 10* sårbarheter som injections, Cross-Site Scripting, Security Misconfigurations och Cross-Site Request Forgery etc.	✓	
Säkerhetshot: Virus**, malware, backdoors, botnet infektioner etc.	✓	
IPv4	✓	
IPv6	✓	
Kontroll inför revision, Compliance: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX		●
Kontroll inför revision, Configuration: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA		●

* För mer information se: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
** Nessus kan detektera symptom på virusangrepp men ersätter inte ett antivirussystem.