maart 2023

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Securitytesten

Kent uw organisatie de kwetsbaarheden in uw informatiesystemen voldoende?

Wat zijn securitytesten?

Vrijwel alle organisaties maken gebruik van informatiesystemen in hun bedrijfsprocessen. Dat betekent dat kwetsbaarheden in informatiesystemen direct of indirect impact kunnen hebben op uw bedrijfsvoering en de continuïteit van uw organisatie. Goed inzicht in kwetsbaarheden levert dus belangrijke informatie op om uw kroonjuwelen te beschermen en risico's adequaat te mitigeren. Om dit inzicht in uw informatiesystemen te krijgen kunt u een securitytest uitvoeren. Dit is een test die u inzicht geeft in deze kwetsbaarheden en u aanvullende zekerheid over de beveiliging van uw informatiesystemen. Voor een goede securitytest is het van belang een goede opdracht te formuleren en gedegen regie te voeren zodat het resultaat ook goed aansluit op uw behoeften. Een goede voorbereiding is dus het halve werk.

Waarom securitytesten?

Als er geen inzicht is in mogelijke kwetsbaarheden, is de kans groot dat een organisatie kwetsbaar is voor cybercriminelen of statelijke actoren zonder dat de organisatie dat weet. Dit kan zeer grote gevolgen hebben voor de bedrijfsvoering. De organisatie kan zijn werk niet meer doen, er ontstaat financiële schade of reputatieschade.

Hoe neemt u securitytesten op in het securityprogramma van uw organisatie?

Stappenplan securitytesten

Stap 1 **Bepaal uw doel**	*Stap 2* **Bepaal het middel**	*Stap 3* **Voer regie over de uitvoering**	*Stap 4* **Borg de verbeteringen in uw organisatie**
Bedenk waarom u een securitytest wilt	*Kies een type securitytest*	*Selecteer een geschikte opdrachtnemer*	*Evalueer de securitytest*
Bepaal wat u waartegen wilt beschermen	*Bepaal de scope en diepgang van de test*	*Stuur de uitvoering van de opdracht*	*Borg de verbeterpunten*
Stel concrete onderzoeksvragen	*Formuleer de opdrachtomschrijving*	*Stuur de oplevering*	*Controleer of de bevindingen zijn opgelost*

Aandachtspunten

1. Stel uzelf de juiste vragen voor een goede doelstelling.
2. Er zijn verschillende aanbieders die verschillende typen securitytests aanbieden die er ook nog verschillende terminologie voor gebruiken. Verklaringen van de diverse termen kunnen teruggevonden worden in het Woordenboek Cyberveilig Nederland.
3. Voer regie over de uitvoering: Begeleid de testers.
4. Door aansluiting te zoeken bij het overkoepelende risicomanagement borgt u de bevindingen in de organisatie.

Zorg dat securitytesten is opgenomen in het securityprogramma zodat er een systematische aanpak ontstaat.

De whitepaper securitytesten is een handleiding die uw organisatie in vier stappen door het proces begeleidt, zodat u de veiligheid van uw informatiesysteem zo goed mogelijk kunt verbeteren.

Whitepaper Securitytesten *(ncsc.nl)*