SECURITY AUDIT

Een diepgaande securitycheck van webapplicaties

Met managed hosting van True weet je dat de infrastructuur waarop jouw webapplicatie draait optimaal is beveiligd, maar hoe staat het met de beveiliging van de webapplicatie zelf? Met de securityaudit van True worden ook de webapplicaties periodiek geaudit op securityissues.

true.nl/securityaudit

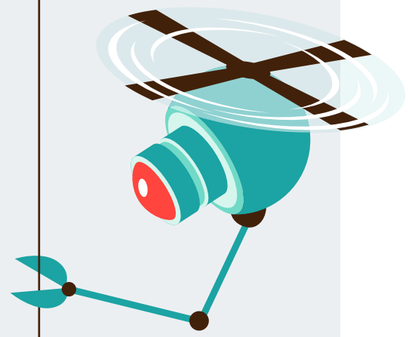
TRUE

Beveiliging van webdiensten wordt steeds urgenter

Dagelijks worden duizenden bedrijven en instellingen, al dan niet automatisch, aangevallen. Deze aanvallen brengen niet alleen schade toe, maar vaker nog wordt bedrijfskritische en concurrentiegevoelige infomatie buit gemaakt. In de ergste gevallen worden persoonsgegevens gelekt, sinds januari 2016 brengt dat niet alleen bedrijfs- en imagoschade met zich mee, maar kan onder deze wet forse boetes tot gevolg hebben.

Met Managed Hosting van True weet u dat uw infraplatform goed is beveiligd tegen deze hedendaagse gevaren, maar hoe staat het eigenlijk met uw webapplicaties en websites? Uw developers zijn de besten in hun vak, maar effectieve en continu geactualiseede applicatie- en systeembeveiliging: is dat ook hun vak? Om u een totaalpakket aan veiligheid en zekerheid te bieden heeft True de True Security Audit. Hiermee krijgt u de zekerheid dat de beveiliging van uw volledige webomgeving met regelmaat grondig tegen het licht wordt gehouden en eventuele bedreigingen vroegijdig kunnen worden geëlimineerd.

True Security Audits onderzoeken op een intensieve en de technologisch meest actuele manier in hoeverre de geaudite website, webapplicatie of webshop omgaat met informatie, welke informatie van buitenaf is op te halen en waar eventuele lekken - om van buitenaf binnen te treden - zich bevinden.



True biedt uitgebreide Security Audits voor webshops, websites, webportals en webapplicaties.

De audit bestaat uit een brede mix van verschillende geautomatiseerde scans, online company infosearches, human attempts en interpretation waarvan de resultaten met hun risicofactoren uitvoerig worden gerapporteerd. Aangezien de gevaren dagelijks toenemen en van vorm veranderen voeren we Audits minimaal twee keer per jaar uit.

De audits worden uitgevoerd door Security Engineers met veel technische kennis en praktijkervaring met ondermeer ethisch hacken.

Na elke Security Audit ontvangt u een uitgebreide rapportage met een overzicht van gevonden lekken en kwetsbaarheden. Aan de hand van de gegeven aanbevelingen kunt u de gevonden zwakheden corrigeren en verbeteren. Middels een rescan worden de zwakheden op een later tijdstip opnieuw onderzocht.

Waarom is het zinvol om voor een Security Audit van True te kiezen?

- → Wees bedreigingen voor
- → Continuiteit voor de organisatie
- → Voorkom verlies van gevoelige data
- → Voorkom bedrijfs- en imagoschade
- → Voorkom boetes voor datalekken

2 type audits voor een veiligere webapplicatie

BLACKBOX (14 UREN)

De meest voorkomende manieren en exploits onderzocht

De security specialist weet bij een blackbox audit niets van de omgeving, de interne structuur of de te testen objecten. De methode is in de meeste gevallen gelijk aan die kwaadwillenden gebruiken voor het binnendringen binnen de applicatie(s). De meest voorkomende manieren en exploits om in te breken binnen websites worden door de specialist gecontroleerd. De blackbox audit wordt uitgevoerd op 1 URL.

GREYBOX (24 UREN)

Uitgebreidere resultaten en inzicht in specifieke kwetsbaarheden

Doel van deze audit is om naast andere kwetsbaarheden ook te onderzoeken of er kwetsbaarheden zijn bij het inloggen als gebruiker. De specialist beschikt hierbij wel over voorkennis van de omgeving. De security specialist gebruikt een standaard account, en extra informatie van de webomgeving. De greybox scan neemt minimaal 24 uren in beslag en focust zich voor een groot deel, naast de reguliere scan, ook op 'human-interpretation'

Kwetsbaarheden scan (OWASP)	●	●
Real life hack situatie	●	●
Datalekken onderzoek (search engine en bekende datalekken)	●	●
Human interpretation (verbanden tussen informatiebronnen)	●	●
Rescan	●	●
POST inlog scan	—	●
Advanced sensor scanning	—	●
Datalekken onderzoek (search engine en uitgebreide datalekkenanalyse)	—	●
Webapplicatie malware scan (beta)	—	●

Kwetsbaarheden en aanbevelingen helder gerapporteerd

Na het uitvoeren van de Security Audit ontvangt u van True een onderzoeksrapport met een overzicht van gevonden kwetsbaarheden en aanbevelingen. Na enkele weken zullen we controleren of uw organisatie de gevonden lekken heeft gedicht. Dit doen we met een Security ReScan. Wanneer u de gevonden lekken na de rescan nog niet verholpen heeft nemen wij contact met u op. Het verhelpen van de specifieke lekken kan in veel gevallen gecompliceerd zijn doordat deze diep in de applicatiecode zit. Wanneer nodig kunnen wij of een van onze partners u helpen met het dichten van het lek.

De hosting van webapplicaties gemanaged

Veel organisaties laten verantwoordelijkheden die de ‘lijm’ tussen de webapplicatie en de infrastructuur moeten vormen in het midden liggen. Of laten de verantwoordelijkheid over aan webontwikkelaars, die de kennis van de volledige technologiestack ontberen of simpelweg te weinig tijd hebben om dit continu te optimaliseren. Daarom heeft True ruim 10 jaar geleden de verantwoordelijkheid voor dat grijze gebied genomen. Profiteer van onze doorontwikkelde systemen, kennis en kunde om jouw webprojecten naar het volgende niveau te tillen.

Ga voor meer informatie naar
true.nl/managedhosting

Postadres
Postbus 51050
1007 EB Amsterdam

Bezoekadres
Keienbergweg 100
1101GH Amsterdam

E-mail
Algemeen: informatie@true.nl
Support: support@true.nl

Telefoon
31 (0)20 305 97 50