SECURITY-AUDIT

Een diepgaande security-audit voor webapplicaties

De beveiliging van je webapplicatie in kaart gebracht:

→ Wees bedreigingen voor met een uitgebreide securitycheck
→ Borg continuïteit voor de IT-operatie in de organisatie
→ Voorkom verlies van gevoelige bedrijfsinformatie
→ Vermijd bedrijfs- en imagoschade
→ Voorkom boetes voor datalekken

Wil je meer informatie over de securityaudit van True?
0800 BEL TRUE of ga naar true.nl/securityaudit

TRUE

Beveiliging van webdiensten wordt steeds urgenter

Met managed hosting van True weet je dat de infrastructuur van het hostingplatform optimaal is beveiligd, maar geldt dat ook voor de beveiliging van jouw webapplicaties die daarop draaien? Met de security-audit scant True periodiek jouw webapplicaties op veelvoorkomende security-issues.

Uitgebreid onderzoek naar kwetsbaarheden in webshops, websites & webapplicaties

De securityaudit bestaat uit een brede mix van geautomatiseerde scans, online onderzoek naar kwetsbaarheden binnen de organisatie en handmatige pogingen om in te breken in systemen en omgevingen.

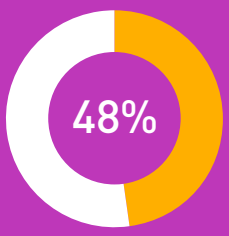
De resultaten van de audit worden zorgvuldig geïnterpreteerd door de onderzoeker, voorzien van een risicoprofiel en vast-gelegd in een rapportage.

De audits worden uitgevoerd door security-engineers met veel technische kennis en praktijkervaring met onder meer ethisch hacken.

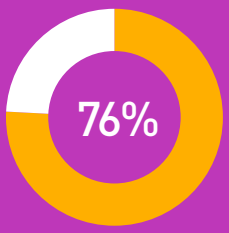
Na afloop ontvangt u een uitgebreid rapport met een overzicht van de gevonden lekken en kwetsbaarheden. In het rapport staan tevens aanbevelingen voor het oplossen van de risico's.

Omdat gevaren dagelijks toenemen en van vorm veranderen, adviseren we om minimaal twee audits per jaar uit te laten voeren.

Onze security-audit in cijfers (2017)

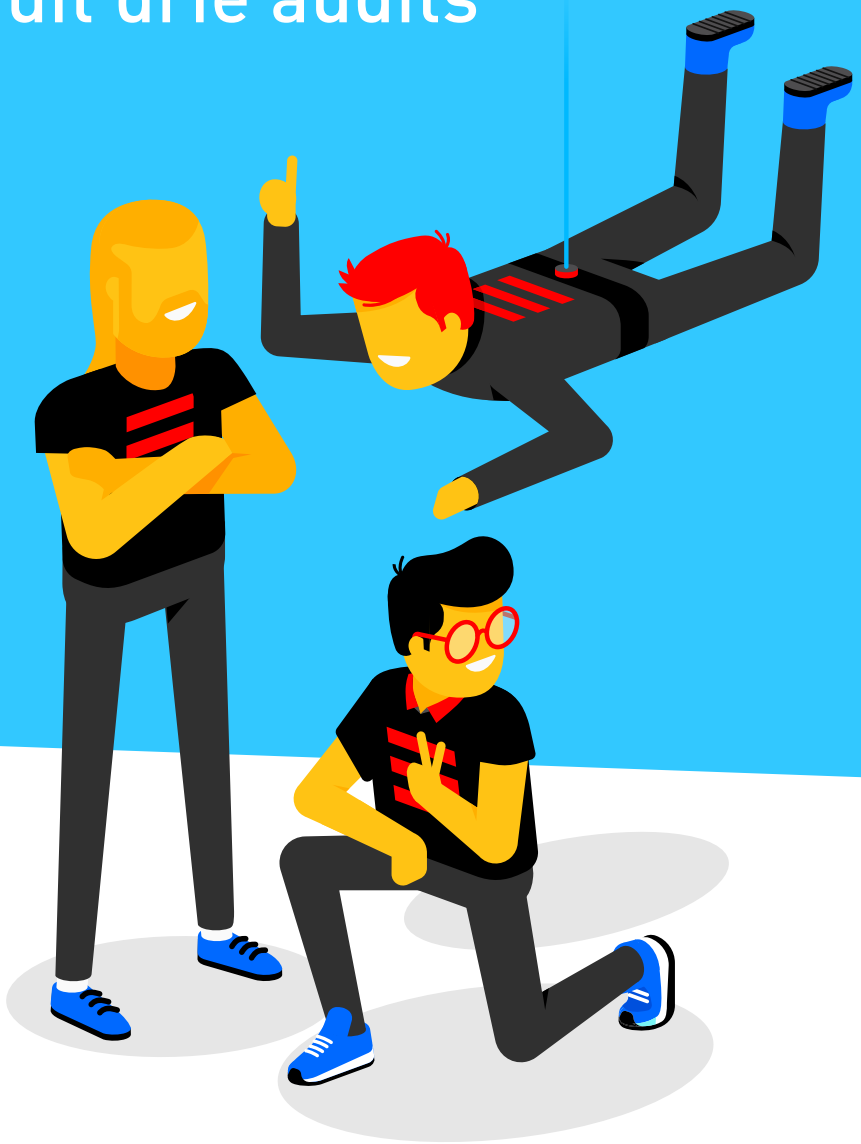


In 48% van de gevallen lukte het onze engineers om het beheer de omgeving volledig over te nemen.



In 76% van de gevallen hadden onze security-engineers toegang tot persoonsgegevens. Bij kritieke gevallen werd vroegtijdig melding gedaan.

Keuze uit drie audits



Lite:
16 uur hacken

Voor organisaties die niet de hele webomgeving willen laten hacken en vooral op zoek zijn naar de technische knelpunten. De security audit is een onderzoek van 16 uur waar uitgebreide inzichten worden gegeven in een voor techneuten leesbaar rapport.

Standard:
32 uur hacken

Een uitgebreid onderzoek waarbij de security-engineer geen voorkennis heeft van de omgeving en ruim 32 uur zal hacken. Naast onderzoek naar veelvoorkomende digitale aanvallen wordt er gekeken of er kwetsbaarheden zijn bij het inloggen als gebruiker. De resultaten worden uitgebreid gedocumenteerd in een adviesrapport.

Enterprise:
64 uur hacken

Voor omgevingen met een erg uitgebreide applicatie waar we ruim-schoots de tijd voor nemen. Inclusief alle extra's zoals bijvoorbeeld de mogelijkheid tot geavanceerde phishingcampagnes en on-site trainingen van white hat hackers.

	Lite	Standard	Enterprise
Security-audit uren (exclusief audit rapport)	16 uur	32 uur	48 uur
Kwetsbaarhedenscan(OWASP)	•	•	•
Real-life hacksituatie	•	•	•
Datalekkenonderzoek (search engine)	•	•	•
Human interpretation (verbanden tussen informatiebronnen)	•	•	•
Webapplicatie malwarescan (beta)	•	•	•
Horizontal escalation (inzien van andere gebruikersgegevens)	•	•	•
Vertical escalation (rechten verhogen)	•	•	•
POST-inlogscan	•	•	•
Datalekken onderzoek (search engine en uitgebreide datalekkenanalyse)	•	•	•
Advanced sensorscanning (PHP- en .NET-applicaties en enkel op acceptatie-omgevingen)*	•		•
Eenvoudige rapportage van de bevindingen (bevinding (technisch), risico-calculatie)	•		
Zeer uitgebreide rapportage van de bevindingen (uitleg, kans, risico, impact, aanbeveling)		•	•
Aanvalscenario's (gecombineerde aanvallen)		•	•
Mogelijkheid tot phishing campagne*			•
Mogelijkheid tot onsite security test*			•
Mogelijkheid tot onsite security training*			•
Standaard aantal audits per jaar (incl. re-scan)	2	2	2

*Deze onderdelen zijn uitsluitend op aanvraag. Vraag naar de mogelijkheden.

Kwetsbaarheden en aanbevelingen helder gerapporteerd

Na het uitvoeren van de securityaudit ontvangt u van True een onderzoeksrapport. In dit rapport vindt u een overzicht van gevonden kwetsbaarheden, risico-analyses en aanbevelingen. Na enige tijd controleren we in een rescan of de gevonden lekken zijn gedicht. Indien de lekken tijdens een rescan nog niet zijn gedicht, nemen wij contact met u op om dit te melden. Het verhelpen van specieke lekken kan in veel gevallen gecompliceerd zijn, omdat deze die in de applicatie kunnen zitten. Heeft u moeite in het verhelpen van een kwetsbaarheid? Dan kan True of een van de partners u verder op weg helpen.

De hoogste veiligheids- en compliance-standaarden

Veilig

Dagelijks speurt ons securityteam naar mogelijke gevaren voor de volledige applicatie-infrastructuur. De experts kijken proactief naar hoe de webomgeving schoon blijft van invloeden van buitenaf.

Compliant

True is ISO 27001, ISO 9001 en NEN 7510 gecertificeerd. Dit betekent dat we onze informatieprocessen in kaart hebben gebracht en uitgebreide beveiligings-maatregelen hebben genomen.

Schaalbaar

Een webomgeving moet snel in kunnen spelen op veranderingen. Onze servers, database-apps en overige middleware zijn snel up-to-date en klaar om wijzigingen door te voeren.

Saving the world from IT-monsters

Het perfecte samenspel tussen webontwikkelaars, security-, netwerk- en systeemspecialisten is al meer dan zeventien jaar onze expertise. Ons team bestaat uit experts die de verantwoordelijkheid nemen over de complete webtechnologiestack. Van infrastructuur tot connectiviteit. Van middleware tot data. Voor managed webomgevingen die zijn ingericht om veiligheid, schaalbaarheid en compliance maximaal te borgen.

Wil je meer informatie over de oplossingen van True?
0800 BEL TRUE of ga naar true.nl/securityaudit

Bezoekadres AMS
Keienbergweg 100
1101GH Amsterdam

Bezoekadres MST
Amerikalaan 1
6199AE Maastricht-Airport

0800 BEL TRUE
info@true.nl
www.true.nl

True is ISO 27001, NEN 7510, ISO 9001, ISO 14001 en ISAE 3402 type I & II gecertificeerd.