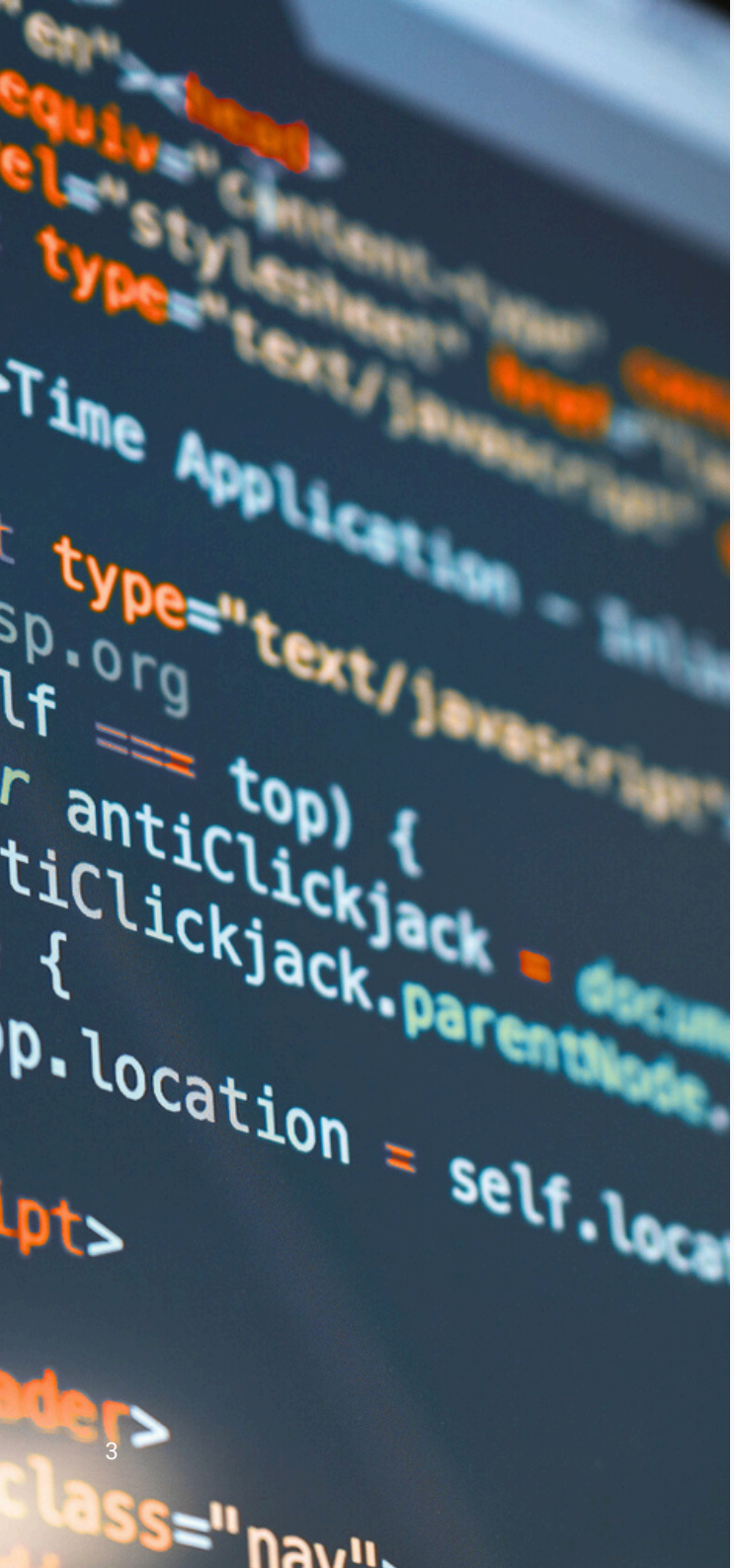
Securify

De kracht van Continuous Pentesting

Waarom de jaarlijkse pentest niet meer voldoet

WHITEPAPER

Inhoud



Introductie

De manier waarop organisaties software en applicaties ontwikkelen is de afgelopen tien jaar volledig veranderd. Teams werken agile en releasen vrijwel continu nieuwe functies. Toch zijn de meeste securityprocessen nauwelijks meegegroeid met deze snelheid. Het klassieke model is gebaseerd op één pentest per jaar. Daarna volgt een rapport en een herstelronde. Dit stamt nog uit de tijd dat softwareontwikkeling voorspelbaar en overzichtelijk was.

Die tijd is voorbij. Voor veel organisaties is de jaarlijkse pentest nog altijd het standaardbewijs dat een applicatie veilig is. Maar een momentopname, hoe grondig ook, garandeert niet dat een applicatie veilig blijft. De realiteit is dat nieuwe releases, updates en integraties vrijwel dagelijks voor nieuwe risico's zorgen.

Als je wilt blijven voldoen aan klantverwachtingen en blijft innoveren, kun je niet zomaar vertrouwen op een proces dat maanden achterloopt op de realiteit. Security moet net zo flexibel, snel en iteratief zijn als de softwareontwikkeling zelf. Bovendien moet je momenteel ook voldoen aan de nieuwste securitystandaarden en regelgeving zoals NIS2 of DORA.

In deze whitepaper ontdek je waarom jaarlijks testen en statische pdf-rapporten niet langer volstaan en hoe je met Continuous Pentesting de stap zet naar een continu, datagedreven proces. Je krijgt inzicht in hoe een realtime securitydashboard kwetsbaarheden signaleert, welke risico's urgent zijn bij nieuwe releases en hoe die informatie automatisch terechtkomt bij je ontwikkelteam. Met een directe security feedbackloop, volgt security automatisch in de slipstream van ontwikkeling.

"Als je wilt blijven voldoen aan **klantverwachtingen** en blijft **innoveren**, kun je niet zomaar vertrouwen op een proces dat maanden achterloopt op de realiteit."

Waarom een jaarlijkse pentest niet meer genoeg is

Testen is essentieel om grip te houden op de veiligheid van digitale systemen. Kwetsbaarheden in applicaties kunnen leiden tot datalekken, verstoring van dienstverlening of reputatieschade. Dat leidt tot ontevreden klanten en financiële schade. Zeker in sectoren waar software cruciaal voor de operatie is of bij applicaties die werken met persoons-, medische of andere gevoelige gegevens. In die gevallen wil je als organisatie kunnen aantonen dat je de risico's kent, beheerst en waar nodig tijdig ingrijpt.

Het traditionele proces voor pentesten sluit daarop aan. Er is een intake om risico's en scenario's in kaart te brengen, de testfase zelf en een rapportage van de bevindingen. Veel organisaties hebben dit proces verankerd in hun beleid of opgenomen in hun compliance-frameworks. Toch levert die aanpak steeds vaker spanning op. De ontwikkelcyclus is veranderd van een handvol releases per jaar naar een continue stroom van nieuwe functionaliteit. Software is heel dynamisch en verandert soms dagelijks. Een testrapport van een paar maanden geleden, hoe volledig ook, zegt weinig over de huidige versie.

Daar komt bij dat applicaties complexer zijn geworden. Veel moderne applicaties zijn opgebouwd uit tientallen losse componenten, vaak ontwikkeld door verschillende teams of leveranciers. Iedere wijziging aan zo'n component kan voor nieuwe kwetsbaarheden zorgen.

Een jaarlijkse pentest zorgt zo voor een vals gevoel van veiligheid. Een goedgekeurde release is geen garantie voor wat er daarna gebeurt. Dit proces lijkt op 'schieten op een bewegend doel'. Als het rapport is opgeleverd, is het bijna alweer achterhaald.

Bovendien zijn aanvallen steeds geavanceerder. Hackers en cybercriminelen zijn beter georganiseerd, hebben meer middelen en maken volop gebruik van geautomatiseerde tools. Zelfs minder ervaren hackers kunnen met standaardsoftware serieuze schade aanrichten. Daardoor zijn kwetsbaarheden sneller te vinden en te misbruiken. De tijd tussen een codewijziging en een daadwerkelijke aanval is korter dan ooit. Security die maanden achterloopt, biedt dan onvoldoende bescherming.

Ook toezichthouders, auditors en klanten stellen steeds vaker kritische vragen. Hoe weet je zeker dat nieuwe functionaliteit veilig is? Hoe borg je dat je risico's op tijd ontdekt? Hoe snel kun je aantonen dat je maatregelen hebt genomen? Veel organisaties kunnen deze vragen niet volledig beantwoorden. De jaarlijkse pentest was jarenlang een minimumnorm, maar dit is niet langer voldoende.

Snelheid als onderscheidend vermogen

Digitale innovatie is niet vrijblijvend. In vrijwel elke sector bepaalt de snelheid waarmee je nieuwe diensten ontwikkelt of je relevant blijft. Banken, verzekeraars, zorgorganisaties en technologiebedrijven concurreren niet alleen op prijs en kwaliteit, maar vooral op hoe snel ze inspelen op veranderende klantbehoeften.

Met Agile development en DevOps is het mogelijk in hoog tempo nieuwe functionaliteit live te brengen. Maar deze snelheid schuurt met klassieke security. Het traditionele testproces vereist telkens opnieuw afstemming, planning, wachttijden en rapportages. Die aanpak vertraagt het ontwikkelproces en levert bovendien geen actueel beeld op. Ontwikkelteams willen geen weken wachten op een testresultaat. Ze willen realtime inzicht, zodat ze kwetsbaarheden direct in de volgende sprint kunnen oplossen. Zolang security een losstaand proces blijft, vertraagt het innovatie. En zolang een pdf-document het bewijs is, heb je nooit zekerheid of je applicatie echt veilig is.

Door wijzigingen in applicaties direct te controleren, zijn mogelijke problemen meteen in de kiem te smoren. Dit voorkomt vervelende verrassingen op het laatste moment en kostbaar herstelwerk. Kortom, door security tests te borgen in het ontwikkelproces kan je sneller reageren en innoveren. Daarnaast zijn de kosten voor herstelwerk lager. Een bug vroeg ontdekken en oplossen is tot 30 maal goedkoper dan een fix vlak voor, of nog erger, pas na go-live.

> “Ontwikkelteams willen **realtime inzicht**, zodat ze kwetsbaarheden direct in de volgende sprint kunnen oplossen.”

Continuous Pentesting: de nieuwe standaard

Security is geen blokkade. Integendeel, het kan een versterker zijn van innovatie als je het op dezelfde manier organiseert als development. Als je testen flexibel, iteratief en continu inzet, is het juist een versneller van innovatie. Daarom is Continuous Pentesting geen verzameling losse tools of een extra laag documentatie, maar een fundamenteel andere manier van werken. In plaats van te vertrouwen op jaarlijkse meetmomenten, wordt security een integraal proces om nieuwe releases realtime te monitoren en risico's voortdurend in te schatten. Bovendien krijgt het ontwikkelteam direct de feedback om problemen op te lossen. De kracht van deze aanpak zit in de combinatie van automatisering, menselijke expertise en een centraal dashboard waarin alles samenkomt.

Van pdf's naar realtime inzicht

Een groot verschil is dat het dashboard de ontwikkelcyclus op de voet volgt. Alle wijzigingen en nieuwe features worden direct gevalideerd. Zo ontstaat een continu beeld in plaats van een periodiek overzicht. Voor CISO's, Product Owners, C-level management en auditoren is dit een goudmijn.

Een belangrijk kenmerk voor ontwikkelteams is dat het direct gekoppeld is aan de ontwikkeltools die teams dagelijks gebruiken. Bevindingen verschijnen automatisch in de backlog. Ontwikkelteams krijgen direct te zien welke nieuwe kwetsbaarheden zijn ontdekt, hoe ernstig ze zijn en waar ze zich in de applicatie bevinden. Elke bevinding bevat alle details, zodat teams direct kunnen starten met het beoordelen en verhelpen ervan. Zo is security geen extra stap, maar een onderdeel van het normale ontwikkelproces.

De voordelen van Continuous Pentesting

- Altijd een centraal en actueel beeld van de risico's
- Snelle signalering, wat belangrijk is en waar actie nodig is.
- Geen hoge herstelkosten achteraf
- Minder handmatige overdracht
- Snellere responstijd voor het oplossen van kwetsbaarheden
- Direct contact met ontwikkelaars rondom security
- Ontwikkelaars gaan veiligere code schrijven door continue feedback
- Gebaseerd op standaarden en aantoonbaar veilig

Machine learning als versneller

Nu softwareontwikkeling sneller gaat dan ooit, kan security niet alleen afhankelijk zijn van handmatige controles. Daarvoor is er simpelweg te veel code en veranderen systemen en applicaties te snel. De inzet van technologie zoals machine learning is daarom onmisbaar om security veel beter de snelheid van softwareontwikkeling te kunnen laten bijbenen. Hiervoor wordt bijvoorbeeld een zelfontwikkelde risk-engine ingezet om op automatische wijze te kunnen voorspellen welke specifieke code wijzigingen het meeste risico geven op de aanwezigheid van kwetsbaarheden. De engine herkent patronen in wat er veranderd is en bepaalt welke onderdelen potentieel gevoelig zijn voor kwetsbaarheden.

Een wijziging in de kleur van een knop zal bijvoorbeeld nauwelijks aandacht vragen, terwijl een wijziging in de loginfunctionaliteit of een publieke API veel meer risico geeft.

Zo'n 10 tot 20% van een applicatie is meestal relevant voor de beveiliging. Door dat deel goed in kaart te brengen en alle wijzigingen direct en grondig te inspecteren, blijft het security fundament solide, zonder veel onnodig testwerk.

Het uitlichten van deze security hot spots is enorm waardevol voor security specialisten om direct in te zoomen op de plekken die er toe doen. En doordat de engine continu leert van de feedback van security specialisten wordt de voorspellende waarde steeds groter.

Deze unieke aanpak is essentieel om security efficiënt en schaalbaar te organiseren en dure specialisten zo slim mogelijk in te zetten. Het credo 'Test less, secure more' is essentieel om security reviews slim en op snelheid te kunnen organiseren.

"De inzet van technologie zoals **machine learning** is onmisbaar om security veel beter de snelheid van softwareontwikkeling te kunnen laten bijbenen."

Een geïntegreerde workflow

In traditionele modellen staat security los van het ontwikkelproces. Continuous Pentesting maakt een einde aan die scheiding. Het dashboard, de forecasting engine en de expertise van securityspecialisten zijn een integraal onderdeel van het ontwikkelproces.

Zodra een team een nieuwe release maakt, start automatisch een analyse. Bevindingen zijn meteen inzichtelijk zodat het team kwetsbaarheden direct kan oppakken. Ook het risico dat fouten zich verspreiden naar andere onderdelen van het systeem is hierdoor kleiner.

Het dashboard is een centraal informatiepunt. Ontwikkelaars, security officers en managers hebben hun eigen toegang en krijgen een helder beeld op maat. Van individuele bevindingen tot trends over langere perioden: alles is continu beschikbaar en actueel. En omdat de securityspecialisten nauw samenwerken met de ontwikkelteams is er ook continu kennisoverdracht. Dit draagt direct bij aan slimmere en betere security door ontwikkelteam; de kwaliteit van applicaties en security neemt toe en het aantal bevindingen daalt.

Aantoonbaar beter voorbereid

Steeds meer organisaties realiseren zich dat compliance niet ophoudt bij een audit of een jaarlijkse check. Toezichthouders vragen niet alleen of je een pentest hebt uitgevoerd, maar vooral hoe je risico's aantoonbaar beheerst. Het securitydashboard maakt dat aantonen eenvoudiger. Iedere bevinding is traceerbaar en iedere oplossing is gelogd. Verder is elke wijziging gekoppeld aan een standaard, zoals de OWASP Top 10 of de OWASP Application Security Verification Standard (ASVS). Zo ontstaat op elk moment een volledig en betrouwbaar overzicht van de securitystatus.

Nieuwe wetgeving zoals NIS2, DORA en de aankomende Cyber Resilience Act (CRA) maken grip op het proces nog belangrijker. Dit stelt strengere eisen aan aantoonbare security. Organisaties moeten kunnen bewijzen dat ze risico's actief beheersen. Niet alleen preventief, maar ook tijdens en na elke release. Waar een jaarlijkse pentest jarenlang voldeed voor bijvoorbeeld ISO27001, leggen deze wetten de lat hoger. Continuous Pentesting helpt om te voldoen aan deze kaders door de beveiligingskwaliteit van een product meetbaar en aantoonbaar te maken. Op elke moment kan bijvoorbeeld een rapport worden uitgedraaid met een overzicht van de actuele security status en de activiteiten die worden uitgevoerd om security continu te borgen.

Het resultaat is minder auditdruk, betere bewijsvoering en je sorteert als organisatie voor op toekomstige verplichtingen. Klanten en toezichthouders verwachten steeds vaker dat security structureel geborgd is. Continuous Pentesting maakt dat niet alleen mogelijk, maar dus ook aantoonbaar.

"Steeds meer organisaties realiseren zich dat **compliance** niet ophoudt bij een **audit** of een jaarlijkse check".

Snel en veilig innoveren

De jaarlijkse pentest was lange tijd de minimumnorm. Maar het minimum is niet langer voldoende. In een wereld waarin software continu verandert, moet security meebewegen.

Continuous Pentesting maakt beveiliging een continu proces, geïntegreerd in hoe organisaties ontwikkelen, releasen en verbeteren. Het is tijd om afscheid te nemen van de klassieke pentest en te kiezen voor een aanpak die aansluit op de snelheid van moderne softwareontwikkeling en het mogelijk maakt om snel én aantoobaar veilig te innoveren. Met realtime zicht op de risico's, van elke release en niet slecht één of twee keer per jaar. Zo wordt security een lopend filmpje in plaats van af en toe een losse foto.

Benieuwd hoe jouw securityproces sneller en slimmer kan?

Ontdek hoe Continuous Pentesting werkt in de praktijk. Neem contact op voor een vrijblijvende demo.

Ervaar zelf waar jouw organisatie nu staat en waar het slimmer, sneller en veiliger kan.

+31(0)20 820 4516

info@securify.nl

Securify

Securify B.V.
Naritaweg 132
1143 CA Amsterdam

T +31(0)20 820 4516
E info@securify.nl
www.securify.nl

Securify helpt organisaties met het identificeren, verhelpen en voorkomen van technische beveiligingsrisico's met pentesten, red teaming opdrachten en security code reviews. De focus ligt hierbij op effectieve beveiliging tegen de grootste bedrijfsrisico's. Op basis van security roadmaps worden code, (mobiele) applicaties, infrastructuur en de organisatie als geheel optimaal beveiligd. Veel bedrijven, van start-ups tot grote banken, vertrouwen al jaren op Securify om hun systemen en (mobiele) applicaties goed te beveiligen. Met honderden penetratietesten en security code reviews per jaar helpt het Securify team de gegevens van miljoenen Nederlanders goed te beveiligen.

Daarnaast voorziet Securify in een innovatieve visie op applicatiebeveiliging van (bedrijfs)kritieke systemen. De unieke aanpak van Securify stelt ontwikkelteams in staat continu, aantoonbaar, sneller én veiliger software te leveren. Op die manier werkt security niet vertragend. Securify is onderdeel van Solvinity Group. Kijk voor meer informatie op **Securify.nl**.