# PKI-AUTOMATISERING: DE STAND VAN ZAKEN IN 2021

# DE STAND VAN ZAKEN OP HET GEBIED VAN PKI-AUTOMATISERING

PKI ligt aan de basis van vrijwel elk aspect van technologie. Het is onmisbaar voor de authenticatie van en ondertekening voor gebruikers, servers, apparaten, het IoT, DevOps-applicaties en -services, digitale documenten en nog veel meer.

Maar het is inmiddels bijna onmogelijk om PKI handmatig te beheren. Uit een recent onderzoek van Ponemon blijkt dat het aantal PKI-certificaten dat bedrijven moeten beheren het afgelopen jaar met 43% is gestegen.[1] In combinatie met de kortere looptijden van certificaten kan dat er al snel toe leiden dat ze hun PKI-certificaatbeheer niet langer in de hand hebben.

Om meer inzicht te krijgen in hoe bedrijven met deze uitdaging omgaan, vroeg DigiCert onderzoeksbedrijf ReRez Research om bij 400 internationale ondernemingen onderzoek te doen onder de IT-managers die verantwoordelijk zijn voor het PKI-beheer. Het resultaat is een totaalbeeld waarin veel onrust heerst, maar waarin tegelijkertijd is te zien hoe de beste organisaties hun PKI-beheer onder controle hebben.

Het aantal PKI-certificaten dat bedrijven moeten beheren, is gestegen met **43%**

## WAT IS PKI-AUTOMATISERING?

Voor de deelnemers aan het onderzoek hebben we PKI-automatisering gedefinieerd als bestaande uit de volgende aspecten:

- Opsporen van bestaande digitale certificaten
- Uitgeven van nieuwe digitale certificaten
- Verlengen van digitale certificaten voordat ze verlopen
- Intrekken van digitale certificaten wanneer nodig
- Automatiseren van codeondertekening
- Registratieproces voor clientcertificaten
- Verifiëren van identiteit (voor bijvoorbeeld documentondertekening)
- Automatiseren van uitgebreide provisioning-activiteiten, zoals invoer in LDAP en Exchange
- Andere onderhoudsactiviteiten op het gebied van PKI-beheer

1 2020 Global PKI and IoT Trends Study (Ponemon)

# DE SNELLE GROEI VAN PKI LEIDT TOT VERWARRING

Gemiddeld beheren de bedrijven in ons onderzoek ruim 50.000 certificaten. De meestvoorkomende certificaattypen zijn gebruikers- en servercertificaten, gevolgd door certificaten voor webservers, mobiele apparaten en e-mail. Bedrijven beheren 33% meer openbare certificaten of certificaten die zijn uitgegeven door een openbare certificaatinstantie (CA), dan persoonlijke certificaten die zijn uitgegeven door een interne certificeringsinstantie.

## Gemiddeld beheren bedrijven nu ruim **50.000** certificaten.

Dit is een aanzienlijke stijging ten opzichte van eerdere jaren en het is duidelijk dat de bedrijven moeite hebben met het vele extra werk dat dit met zich meebrengt. Twee derde van hen heeft te maken gehad met uitval als gevolg van onverwacht verlopen certificaten. Bij een op de vier kwam die uitval vijf tot zes keer voor in alleen al het afgelopen halfjaar.

Hoe kan dat? Deels is dit het gevolg van de toegenomen werkdruk. Bijna twee derde van de bedrijven maakt zich enigszins tot ernstig zorgen over de hoeveelheid tijd die wordt besteed aan het beheren van certificaten. Daarnaast is er het gebrek aan zichtbaarheid. Bij 37% van de bedrijven houden drie of meer afdelingen zich bezig met certificaatbeheer, met onduidelijkheid en verwarring tot gevolg. Bij de meeste bedrijven worden er tot wel 1200 certificaten eigenlijk niet beheerd. Bij ongeveer de helft van hen (47%) worden regelmatig ongeautoriseerde certificaten ontdekt; dat zijn certificaten die zijn geïmplementeerd zonder medeweten van en zonder beheer door de IT-afdeling. Een voor de hand liggende oplossing voor deze problemen is het automatiseren van PKI; daarom hebben we gekeken naar de mate waarin bedrijven daarmee bezig zijn.

**61%** MAAKT ZICH ZORGEN OVER DE BENODIGDE TIJD VOOR CERTIFICAATBEHEER

**47%** VINDT REGELMATIG ONGEAUTORISEERDE CERTIFICATEN

**37%** HEEFT 3 OF MEER AFDELINGEN DIE CERTIFICATEN BEHEREN

**1 IN 4** HAD TE MAKEN MET 5-6 GEVALLEN VAN PKI-GERELATEERDE UITVAL IN DE AFGELOPEN ZES MAANDEN

# 91% VAN DE ONDERNEMINGEN HEEFT BEHOEFTE AAN PKI-AUTOMATISERING

Uit ons onderzoek blijkt dat er bij veruit de meeste bedrijven (91%) op zijn minst gesproken wordt over het automatiseren van PKI. Slecht 9% zegt dat PKI-automatisering geen discussiepunt is en er ook geen plannen voor zijn. De meerderheid van de bedrijven (70%) verwacht binnen een jaar een oplossing te implementeren. Een kwart is in het stadium dat ze al bezig zijn met de implementatie van een oplossing, of die zelfs al hebben afgerond. Eenvoudig is het zeker niet. De uitdagingen die worden genoemd, zijn onder andere hoge automatiseringskosten, complexiteit, complianceproblemen en weerstand tegen veranderingen bij zowel medewerkers als leidinggevenden.

## TRENDS

Veelgenoemde redenen voor PKI-automatisering:

1. Ongeautoriseerde certificaten
2. Gereedheid voor post-quantumcomputers
3. Veel hogere werkdruk door snel korter wordende geldigheidsduur van certificaten
4. Snelle stijging van het aantal certificaten dat moet worden beheerd
5. Toename van thuiswerk

## PIJNPUNTEN

Beveiligingsproblemen die bedrijven aanzetten tot automatisering:

1. Trage provisioning van nieuwe certificaten
2. Verkeerde configuratie van certificaten
3. Overbelaste medewerkers
4. Te veel ongeautoriseerde certificaten
5. Gemiste verloopdatums van certificaten
6. Langzame of mislukte intrekking van certificaten wanneer nodig

## NEGATIEVE GEVOLGEN

De negatieve kosten van het niet automatiseren van PKI:

1. Complianceproblemen
2. Beveiligingsproblemen
3. Kosten
4. Downtime
5. Ontevreden klanten of medewerkers

## DOELEN

Bedrijven die PKI-automatisering implementeren, willen:

1. Beveiliging verbeteren
2. Compliance verbeteren
3. Wendbaarheid verbeteren
4. Productiviteit verbeteren
5. Downtime en kosten verminderen

# DE BESTEN VERSUS DE SLECHTSTEN

We hebben een reeks vragen gesteld om te bepalen hoe goed of slecht elke deelnemer het deed met betrekking tot uiteenlopende PKI-aspecten:

- Voorkomen van downtime door onverwacht verlopen certificaten
- Snel certificaten intrekken wanneer dat nodig is
- Efficiëntie van het beheer van digitale certificaten
- Minimaliseren van beveiligingsrisico's als gevolg van gebrekkig certificaatbeheer
- Complianceproblemen als gevolg van gebrekkig certificaatbeheer
- Minimaliseren van het aantal ongeautoriseerde certificaten
- Voldoen aan SLA's op het gebied van PKI
- Snelheid van uitgifte en intrekking

Aan elk antwoord is een positieve of negatieve score toegekend op basis van hoe goed of slecht ze het deden. Daarna zijn de scores opgeteld.

Om de verschillen inzichtelijk te maken, hebben we de deelnemers in drie groepen verdeeld:

1 **KOPLOPERS**

Dit zijn de organisaties die over het geheel het beste scoorden op de hierboven genoemde criteria.

2 **MIDDENMOOT**

Dit zijn de organisaties die over het geheel gemiddeld scoorden op de hierboven genoemde criteria.

3 **ACHTERBLIJVERS**

Dit zijn de organisaties die over het geheel het laagste scoorden op de hierboven genoemde criteria.

Vervolgens hebben we de koplopers en achterblijvers vergeleken om te zien wat de koplopers anders doen.

# VOOROPLOPEN OF ACHTERBLIJVEN

De deelnemers waren openhartig over hun uitdagingen op het gebied van PKI-beheer. Ze hebben te maken met ongeautoriseerde certificaten, uitval door certificaten die onverwacht verlopen en diverse andere problemen. Maar de problemen zijn niet overal even ernstig. We hebben de antwoorden in drie niveaus verdeeld en de hoogst scorende bedrijven vergeleken met de laagst scorende. De verschillen waren opmerkelijk.

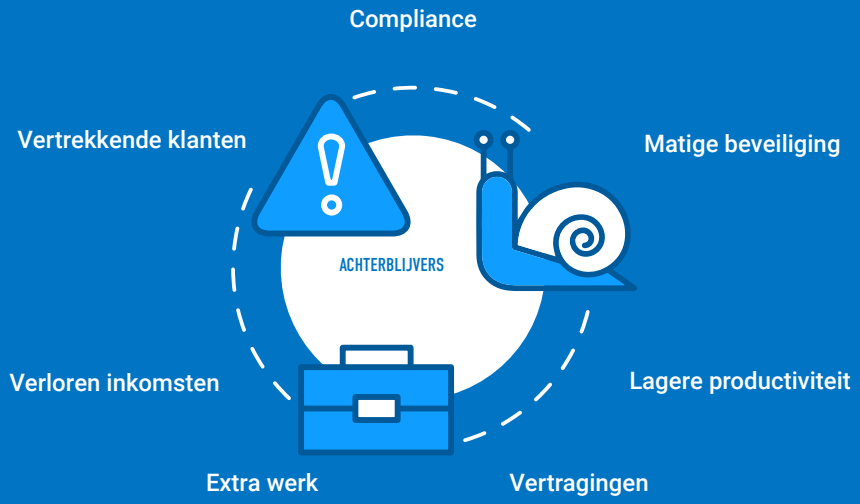
De koplopers doen het simpelweg beter. Opvallend is dat een derde van hen PKI-automatisering sowieso al belangrijker lijkt te vinden. De koplopers zijn twee tot drie keer beter in het:

- Minimaliseren van PKI-beveiligingsrisico's
- Voorkomen van PKI-downtime
- Minimaliseren van ongeautoriseerde certificaten
- Voldoen aan PKI-SLA's
- Beheren van digitale certificaten
- Uitgeven en intrekken van certificaten
- Compliance met wet- en regelgeving

Aan de andere kant ondervinden de achterblijvers ernstige negatieve gevolgen van hun gebrekkige beheer van PKI-certificaten. Die nadelen zijn:

- Complianceproblemen
- Beveiligingsproblemen
- Lagere productiviteit
- Vertragingen
- Te hoge werkdruk
- Verlies van klanten
- Verlies van inkomsten

Maar wat maakt een bedrijf een koploper? En kunnen we iets van deze PKI-koplopers leren?

# PKI-AUTOMATISERING: KENMERKEN VAN DE KOPLOPERS

PKI-koplopers maken zich twee keer zo druk over de tijd die het kost om PKI-certificaten te beheren. Daardoor blijft dit onderwerp onder de aandacht. Ook maken ze zich meer zorgen over ongeautoriseerde certificaten. Ten slotte beschouwen ze PKI-automatisering als een belangrijk aspect van de toekomst van de organisatie. Dat is waarschijnlijk de reden waarom ze zes keer zo vaak PKI-automatisering al hebben geïmplementeerd. Wat kunnen we van hen leren, en wat zou u anders moeten doen?

## HET 'WILDE WESTEN'-EFFECT

Bij het bestuderen van de gegevens vonden we iets interessants. Het bleek dat bedrijven waar het PKI-certificaatbeheer in theorie eenvoudiger zou moeten zijn, in de praktijk juist tegen meer problemen opliepen.

Bijvoorbeeld: bedrijven met het laagste aantal certificaten hadden vaker te maken gehad met uitval als gevolg van verlopen certificaten. Ook scoorden ze consistent lager op allerlei PKI-criteria.

Hierdoor maakten deze bedrijven, met hun lage aantallen certificaten, zich veel meer zorgen over PKI-beheer, ondanks dat ze veel minder certificaten beheerden dan sommige grote ondernemingen. Zo waren ze bijna 50% meer geneigd om te zeggen dat ze zich zorgen maakten over de benodigde tijd voor PKI-beheer. Ook was het aandeel van hun certificaten dat ze beheerden via PKI-automatisering bijna twee maal groter.

Dit lijkt op het eerste gezicht met elkaar in tegenspraak. De realiteit is echter dat het PKI-beheer in deze bedrijven, met hun lage aantallen certificaten, simpelweg minder volwassen is. Bij ondernemingen waar vaak meer dan 100.000 certificaten in gebruik zijn, is het PKI-beheer inmiddels van een zeer hoog niveau. In bedrijven met lage aantallen certificaten is de situatie te vergelijken met het wilde westen: er zijn weinig regels en iedereen doet het op zijn eigen manier.

> IN BEDRIJVEN MET LAGE AANTALLEN CERTIFICATEN IS DE SITUATIE TE VERGELIJKEN MET HET WILDE WESTEN: ER ZIJN WEINIG REGELS EN IEDEREEN DOET HET OP ZIJN EIGEN MANIER.

# PKI-AUTOMATISERING: KENMERKEN VAN DE KOPLOPERS

De koplopers op het gebied van PKI-beheer namen veel meer verantwoordelijkheid voor hun certificaatinventaris, en dachten tegelijkertijd dat ze het slechter deden dan de bedrijven die zich er minder druk om maakten. Maar deze bedrijven hadden juist minder te maken met ongeautoriseerde certificaten en uitval met betrekking tot certificaten, en deden het dus feitelijk veel beter dan ze dachten.

## DE PARADOX VAN DE ZELFBEOORDELING

Een andere interessante bevinding is het zelfbeeld van de bedrijven die zich het meeste zorgen maken over PKI-certificaatbeheer. Die hadden objectief gezien de minste problemen, maar dachten zelf dat ze het niet zo best deden.

Neem bijvoorbeeld de bedrijven die het meest geneigd waren hun PKI-beheer als problematisch te zien. Deze bedrijven zeiden drie tot vijf vaker dat ze zich enigszins tot extreem zorgen maakten over zaken zoals de uitgiftesnelheid voor nieuwe certificaten, verkeerde configuraties, ongeautoriseerde certificaten en andere certificaatproblemen.

En toch waren er bij die bedrijven veel minder ongeautoriseerde certificaten daadwerkelijk aanwezig – slechts twee derde van het aantal ongeautoriseerde certificaten in bedrijven die zich juist geen zorgen maakten. Ook meldden ze minder gevallen van uitval door verlopen certificaten: slechts één geval in zes maanden ten opzichte van drie tot vijf gevallen bij de minder bezorgde bedrijven.

Dit fenomeen zien we vaker in onderzoeken naar beveiliging. Het komt er dus op neer dat deze organisaties hun tekortkomingen en misstappen het nauwkeurigst in de gaten houden en zichzelf er strenger op afrekenen dan bedrijven die er minder aandacht aan besteden. Maar juist doordat ze zo nauwlettend te werk gaan, doen ze het juist veel beter dan de andere.

> BEDRIJVEN DIE ZICH ZORGEN MAKEN OVER PKI-CERTIFICAATBEHEER HADDEN OBJECTIEF GEZIEN DE MINSTE PROBLEMEN, MAAR DACHTEN ZELF DAT ZE HET NIET ZO BEST DEDEN.

# ONZE AANBEVELINGEN

Een consistent gebruik van automatisering voor al uw PKI-certificaten is een onmisbare basis voor organisaties die de controle willen houden over hun cryptografische activiteiten, het aantal menselijke fouten willen terugdringen en de certificaten binnen het bedrijf effectief willen beheren. Maar hoe kunt u de certificaatinfrastructuur met succes automatiseren en beheren? Hier volgt een checklist met aanbevolen stappen.

## 1 IDENTIFICEREN

- Zorg voor een baseline van alle uitgegeven certificaten
- Weet waar alle certificaten zijn geïnstalleerd
- Identificeer alle gebruikers en apparaten die eigenaar zijn van certificaten en domeinen
- Identificeer de besturingssystemen van webservers en de versies van applicaties
- Lokaliseer de cipher suites van webservers en de TLS/SSL-versies

## 2 OPSCHONEN

- Verwijder zwakke sleutels, cipher suites en hashes
- Beperk de uitgifte en verspreiding van wildcard-certificaten
- Implementeer de juiste certificaattypen
- Beperk het aantal standaardcertificaten van leveranciers
- Zorg dat alle webservices zijn voorzien van de laatste patch

## 3 BESCHERMEN

- Standaardiseer en automatiseer de registratie, uitgifte en verlenging
- Installeer en vervang alle certificaten tijdig
- Zorg dat persoonlijke sleutels niet worden hergebruikt bij het verlengen van certificaten
- Installeer certificaten en persoonlijke sleutels op een veilige manier
- Zorg dat certificaten worden verwijderd en ingetrokken wanneer ze niet meer worden gebruikt

## 4 BEWAKEN

- Scan netwerken op nieuwe systemen en wijzigingen
- Controleer de Certificate Transparency-logboeken op ongeautoriseerde TLS-certificaten
- Gebruik CAA om ongeautoriseerde aanvragen voor openbare TLS-certificaten te voorkomen

# WERKWIJZE

Het in Dallas, Texas gevestigde bedrijf ReRez Research hield dit onderzoek onder IT-professionals bij 400 bedrijven van 1000 of meer medewerkers in Noord-Amerika, EMEA, Asia Pacific en Latijns-Amerika. Onder de respondenten bevonden zich IT-directeuren, IT-securitymanagers en IT-generalisten. We bevroegen IT-specialisten die zich bezighouden met het beheer van digitale certificaten voor gebruikers, servers en mobiele apparaten in kleine, middelgrote en grote ondernemingen.

**Praat met een specialist op het gebied van PKI-automatisering van DigiCert over de behoeften en mogelijke maatwerkoplossingen voor uw organisatie. U vindt hier meer informatie over hoe u kunt beginnen met het automatiseren van uw PKI-implementaties.**