TNO innovation for life

Quantum risicomethodologie voor cryptografie

TNO Public ⟩ TNO 2024 R10707
2 mei 2024

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2024 R10707 – 2 mei 2024

Quantum risicomethodologie voor cryptografie

Auteurs	M. de Vries, S.E. Bootsma, V. A. Dunning, M.J. van Vliet
Rubricering rapport	TNO Public
Titel	TNO Public
Rapporttekst	TNO Public
Bijlagen	TNO Public
Aantal pagina's	26 (excl. voor- en achterblad)
Aantal bijlagen	3
Opdrachtgever	Ministerie I&W
Projectnummer	060.57923

Inhoudsopgave

Inhoudsopgave 3
1 Inleiding 4
1.1 Het PQC-handboek 4
1.2 Noodzaak quantum risicobeoordeling 4
2 Quantum risicobeoordeling 5
2.1 Bestaande methodologieën 5
2.2 Deze methodologie 5
2.3 Cryptografische inventaris 6
2.4 Cryptografische kwetsbaarheid 8
2.4.1 Kwetsbaarheidsscore per gevonden algoritme 8
2.4.2 Kwetsbaarheidsscore per applicatie 9
2.5 Impact analyse 10
2.6 Migratie-moeite 14
2.7 Het bepalen van risicoscores 16

Bijlagen

Bijlage A: Checklist cryptografie locaties 19
Bijlage B: Checklist cryptografische inventaris 22
Bijlage C: Kwetsbaarheidsscores voor veelvoorkomende algoritmes 25

1 Inleiding

Quantum computing vormt een potentiële dreiging voor de huidige cryptografie. Deze dreiging raakt echter niet alle cryptografische algoritmes en toepassingen gelijk. Dit document introduceert een methodologie die is ontworpen door TNO om het risico te evalueren waarmee bedrijven worden geconfronteerd in de toekomst. Het stelt een systematische én simpele benadering voor om een cryptografische inventaris te maken en deze te toetsen op zijn kwetsbaarheid voor quantumaanvallen.

De methodologie maakt gebruik van een risicoscore-systeem dat rekening houdt met de bestendigheid of kwetsbaarheid van bestaande cryptografische algoritmen tegen quantumaanvallen, de impact die de aanval zou hebben op het systeem, en de inspanning die nodig is voor de overgang naar quantum-bestendige oplossingen.
Daarnaast is gepoogd om deze risicobeoordeling toegankelijk te maken voor een breder publiek, inclusief degenen met beperkte expertise in cryptografie, bijvoorbeeld door middel van flowcharts en een stapsgewijze handleiding door het proces.

Dit initiatief heeft als doel bedrijven voor te bereiden op een toekomst waarin quantum computing mogelijk de huidige versleutelingsmethoden kan breken, op een doelgerichte manier: met een goede risicoinschatting kan beter worden geprioriteerd en zowel de risico's als de migratiekosten worden beperkt.

1.1 Het PQC-handboek

In december 2023 publiceerde TNO, in samenwerking met de AIVD en het CWI, het PQC-handboek [1]. Dit handboek biedt organisaties richtlijnen voor het migreren naar *post-quantum cryptografie*. Het bevat een concreet stappenplan voor het proces van de migratie, waarbij grofweg drie hoofdstappen worden doorlopen: het stellen van een diagnose, het plannen van de migratie en het uitvoeren van de migratie. De methodologie in dit document probeert organisaties handvaten te geven voor het eerste deel van het proces: het stellen van de diagnose.

Voor het uitvoeren van de diagnosestap, die tot doel heeft de kwetsbaarheid van een organisatie vast te stellen, is het cruciaal om een inventaris te maken en een *quantum risicobeoordeling* uit te voeren. In dit document zullen we dieper ingaan op deze beoordeling. Deze methodologie is een uitwerking van de diagnose stap van het handboek, en voor diepere informatie over algoritmes, type organisaties en quantum resistente alternatieven verwijzen we naar het handboek.

1.2 Noodzaak quantum risicobeoordeling

De noodzaak van een quantum risicobeoordeling hangt af van de organisatie. Om te bepalen of een quantum risicobeoordeling op dit moment nuttig is voor uw organisatie verwijzen wij naar de persona's in het handboek [1]. In dit document gaan we ervan uit dat de conclusie is getrokken dat een quantum risicobeoordeling noodzakelijk is.

2 Quantum risicobeoordeling

2.1 Bestaande methodologieën

In de literatuur vind je diverse methodologieën om quantum risico's te beoordelen. Een van de bekendste benaderingen is Mosca's theorie [2], die stelt dat X+Y > Z moet zijn om goed genoeg voorbereid te zijn op een post-quantumwereld, waarbij:

- X staat voor "Het aantal jaren dat informatie beschermd moet worden",
- Y staat voor "Het aantal jaren dat de migratie duurt", en
- Z staat voor "Het aantal jaren voordat relevante bedreigingen met betrekking tot quantumcomputers zich voordoen".

Een andere benadering is het Wells Fargo-model [3], dat zich voornamelijk richt op drie aspecten: afhankelijkheden tussen componenten, impact en kosten voor oplossingen. Een derde methode is CARAF [4], vooral gericht op "crypto-agility", waarbij de nadruk ligt op het vermogen van een organisatie om zich gemakkelijk aan te passen aan veranderingen in het cryptografische landschap.

2.2 Deze methodologie

Onze aanpak voor het beoordelen van quantumrisico's is een samensmelting van deze benaderingen. Waar de eerder genoemde modellen zich vooral richten op de juistheid van het model, hebben wij juist gestreefd naar een overzichtelijk en praktisch bruikbaar document.

Ons stappenplan om tot een beoordeling van quantumrisico's te komen omvat de volgende stappen:

1. Het maken van een **inventaris** van gebruikte cryptografie.
2. Een koppeling van een quantum **kwetsbaarheid** aan de gevonden cryptografische algoritmes en een vertaling naar cryptografische kwetsbaarheid op systeem/applicatie niveau.
3. Een beoordeling van de **impact** die een quantum computer zal hebben op de organisatie in het algemeen en de systemen in het bijzonder.
4. Een analyse van de **tijd en moeite** die nodig zijn om over te stappen naar post-quantum cryptografie.

Deze 4 stappen zullen stapsgewijs worden behandeld in de volgende hoofdstukken.
Stap 1 dient om de informatie te verzamelen voor de rest van de impact beoordeling. Vervolgens volgt uit stap 2 tot en met 4 telkens een score op 3 niveaus. Deze niveaus zijn door ons opgesteld met als doel om overzichtelijk te blijven. In het geval van kwetsbaarheid is dit gebaseerd op de termijn waarop de cryptografie gebroken wordt (korte termijn, lange termijn, of niet). Voor impact zijn de niveaus gebaseerd op basis van inzicht in de gevolgen voor een organisatie als cryptografie gebroken wordt, rekening houdend met het doel

waarvoor de cryptografie gebruikt wordt. Tot slot is het onderscheid bij de migratie-moeite primair gemaakt op basis van bekende uitdagingen en ervaringen met eerdere migraties.

Na het doorlopen van deze stappen kan het **totale risiconiveau** worden berekend. Dit combineert de scores van kwetsbaarheid, impact en migratie-moeite. Afhankelijk van de combinatie van de drie scores volgt er een totaal risiconiveau welke is onderverdeeld in vijf niveaus: geen risico (0), laag risico (1), gemiddeld risico (2), hoog risico (3) en acuut risico (4). Deze scores zijn gebaseerd op onze inschatting van de prioriteit die gegeven zou moeten worden aan het mitigeren van de risico's.

2.3 Cryptografische inventaris

Het opstellen van een quantum risicoanalyse begint met kennis over welke cryptografie gebruikt wordt. Het maken van een cryptografische inventaris is daarom vaak zowel het belangrijkste als het meest uitdagende onderdeel van de risicoanalyse. Om dit proces te ondersteunen, heeft TNO drie hulpmiddelen ontwikkeld: een checklist over cryptografie gebruik, een checklist over de inhoud van een cryptografische inventaris en een voorbeeld inventaris.

De eerste uitdaging van het inventariseren van cryptografie is het vinden van de cryptografie: het zit in alle uithoeken van een organisatie, ook op plekken waar het niet wordt verwacht: van de printer tot de toegangspoortjes. bijlage a biedt een overzicht waar cryptografie aanwezig zou kunnen zijn. Het geeft ook aanwijzingen waar informatie *over* de cryptografie te vinden kan zijn. bijlage bis een checklist wat er ten minste in een cryptografische inventaris moet zijn geregistreerd. De bijlage geeft ook informatie over de inzet van een inventaris voor andere doeleinden dan een quantum risicoanalyse.

Beide checklists zijn zorgvuldig samengesteld, maar dienen enkel als hulpmiddel: elke organisatie hanteert zijn eigen systemen en methoden. De hier gegeven richtlijnen zijn bedoeld als handreiking, en het is van belang dat een interne expert, zoals een security officer, meekijkt om ervoor te zorgen dat de scope van systemen volledig is.

Deze methodologie dicteert niet *op welke manier* de inventaris gevuld wordt. Dit kan handmatig, bijvoorbeeld als onderdeel van een bestaand security of privacy proces, maar ook (deels) geautomatiseerd, bijvoorbeeld door middel van scanners.

Als derde hulpmiddel hebben we een voorbeeld inventaris vrijgegeven, als bijgevoegd Excel document: **Voorbeeld_Cryptografische_Inventaris.xlsx.**
Deze is ontworpen om het proces van het documenteren van cryptografie te illustreren. We raden met klem aan om de inventaris aan te laten sluiten bij de reeds aanwezige security systemen, ISMS, of ITSM/CMDB. Er zijn ook varianten op de SBOM (Software Bill of Materials), de zogenoemde CBOM (Cryptography Bill of Materials[1]), die geschikt zijn als er gebruik wordt gemaakt van automatische detectie van gebruikte cryptografie.

In dit document zullen we voorbeelden uit de voorbeeld Excel inventaris weergeven in een grijs kader.

[1] GitHub - IBM/CBOM: Cryptography Bill of Materials

Voorbeeld_Cryptografische_Inventaris.xlsx:

In het *Systemen*-tabblad kunnen de gegevens van de IT/OT systemen worden ingevuld., Hier wordt ook de uiteindelijke risicoscore zichtbaar. Impact en migratie-moeite worden doorgaans op systeem niveau bepaald, en in dit voorbeeld daarom hier ingevuld. Het cryptografisch risico wordt automatisch berekend vanuit de gegevens uit het tweede tabblad.

In het tabblad *Cryptografische Inventaris* wordt de specifieke cryptografische informatie voor elk systeem per algoritme ingevoerd. Vaak bevat één systeem meerdere cryptografische algoritmes. Voor de meest voorkomende algoritmes wordt de algoritme risicoscore automatisch ingevuld. Hoe dit berekend wordt, wordt uitgelegd in de komende secties.

Om een cryptografische risicoanalyse uit te voeren, is het van belang om de volgende informatie in ieder geval te registreren:

a. Een uniek identificeerbare naam voor het systeem/code/applicatie dat de cryptografie gebruikt.
b. De daarin gebruikte cryptografische algoritmes.
c. De bijbehorende sleutellengtes (indien van toepassing).
d. Het aantal bits van de hashfunctie outputs (indien van toepassing).

Hybride algoritmes:
Bij het opstellen van een inventaris is het handig om (alvast) rekening te houden met hybride gebruik van algoritmes. Bij hybride algoritmes worden twee algoritmes tegelijkertijd gebruikt voor dezelfde taak, waarbij de output wordt gecombineerd (een huidig algoritme met een PQC algoritme, bijvoorbeeld RSA met Crystals-Kyber), met het idee dat als één van de twee lagen kwetsbaar is (al dan niet door de quantum computer) de andere laag stand houdt. Bij (correct) hybride gebruik is er geen keuze tussen de algoritmes; **beide moeten worden gebruikt.** Dit in tegenstelling tot cipher suites waarbij uit meerdere algoritmes gekozen kan worden.
Het risico wordt met hybride algoritmes verlaagd. Omdat we in de toekomst steeds meer hybride implementaties zullen zien nemen wordt hybride algoritme gebruik ondersteund in de berekeningen.

Voorbeeld_Cryptografische_Inventaris.xlsx:

Hybride gebruik van twee algoritmes kan in het tabblad *Cryptografische Inventaris* worden aangegeven door “In gebruik in hybride vorm? (Ja/Nee)” op “Ja” te zetten en het tweede algoritme in kolom I, K en M in te vullen. De risicoscore houdt hiermee rekening.

Let op: hybride is een speciaal geval: de meeste systemen gebruiken meerdere algoritmes, of bieden meerdere algoritmes opties aan, maar deze worden niet gelaagd zoals in bovenstaande uitleg. Deze algoritmes dienen als separate algoritmes te worden geregistreerd.

2.4 Cryptografische kwetsbaarheid

2.4.1 Kwetsbaarheidsscore per gevonden algoritme

Nadat de cryptografische inventaris is voltooid, moet er een kwetsbaarheidsscore bepaald worden van de gevonden algoritmes. tabel c.5 in bijlage C bevat een overzicht van veel voorkomende algoritmes en hun kwetsbaarheidsscore.

Voor elk algoritme zijn er drie verschillende risiconiveaus:

0. Risicoscore 0 betekent dat het gebruikte algoritme op dit moment *quantum-veilig* is. Het algoritme hoeft volgens de bestaande kennis niet vervangen te worden.
1. Risicoscore 1 betekent dat het gebruikte algoritme nog niet cryptografisch gebroken[2] is, maar dat er wel maatregelen genomen moeten worden. Hoewel dit niveau in theorie niet veilig is, heeft het niet dezelfde urgentie als niveau 2.
2. Risicoscore 2 betekent dat het gebruikte algoritme niet langer veilig is vanwege de opkomst van quantum computers. Het algoritme moet worden vervangen door een quantum resistent alternatief.

De algoritme scores beschouwen alleen de *quantum* kwetsbaarheid. Sommige algoritmes zijn ook vandaag al niet meer veilig door bekende zwakheden. In tabel c.5 wordt dit in een aparte kolom aangegeven. Het is een keuze per organisatie of “huidige zwakheden” meegenomen wordt in de inventaris.

Toelichting risicoscore 1:

Onder risicoscore 1 vallen algoritmes die wel impact hebben van de quantum computer in de toekomst, maar waarbij deze impact beperkt is, en kan worden gemitigeerd met aanpassingen zoals het gebruik van langere sleutels of langere hashfunctie output. *Het algoritme zelf* hoeft dus niet vervangen te worden. Een voorbeeld hiervan is AES met een 128 bits sleutel. Hierbij kan de quantum computer in theorie de veiligheid met de helft verlagen, wat gecompenseerd kan worden met het verdubbelen van de sleutel lengte.

Deze kwetsbaarheden zijn ook minder urgent, het moment van impact ligt verder in de toekomst, dan de kwetsbaarheden op bijvoorbeeld RSA en ECC, die al eerder door quantum computers gebroken kunnen worden.

Tabel 2.1: Voorbeeld cryptografische quantum kwetsbaarheid score per gevonden algoritme

Applicatie	Algoritme	Sleutellengte/ hashlengte	Score
Applicatie A	RSA	2048	2
Applicatie B	RSA	4096	2
Applicatie B	SHA2	256	0
Applicatie B	AES	128	1

[2] Met de term *cryptografisch gebroken* bedoelen wij het feit dat er een wiskundig gezien efficiënte aanval is op het algoritme, die niet verholpen kan worden door bijvoorbeeld een verdubbeling van de sleutellengte.

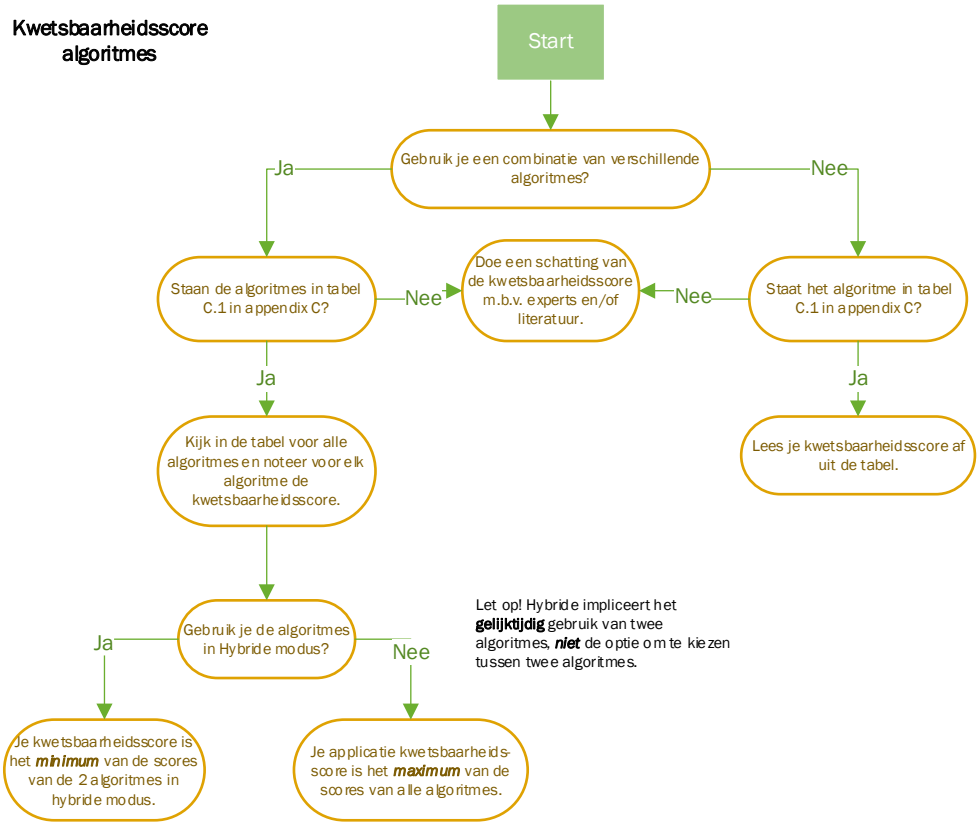
Voorbeeld_Cryptografische_Inventaris.xlsx:

Voor bekende algoritme-sleutellengte/hashfunctie output koppelt de kolom *Quantum kwetsbaarheid* in *Voorbeeld_Cryptografische_Inventaris.xlsx* automatisch de correcte score.

De kwetsbaarheid van algoritmes is geen statisch gegeven. Nieuwe kwetsbaarheden in algoritmes kunnen worden ontdekt. Wij raden daarom aan om periodiek de kwetsbaarheidsscores (bijlage c) te herzien.

2.4.2 Kwetsbaarheidsscore per applicatie

De kwetsbaarheidsscore per applicatie/systeem/server wordt bepaald door de combinatie van kwetsbaarheidsscores van de gebruikte algoritmes in de applicatie.



Figuur 2.1: Flowchart om het totale cryptografische risico per systeem te bepalen.

Met behulp van de flowchart in figuur 2.1 kan men bepalen wat de uiteindelijke risicoscore per applicatie/server/systeem is. Over het algemeen is de applicatie score het *maximum* van de scores van de cryptografische algoritmes in de applicatie: het systeem is zo kwetsbaar als zijn zwakste component. Als je applicatie bijvoorbeeld RSA en AES-128 gebruikt, dan is de risicoscore het maximum van de afzonderlijke kwetsbaarheidsscores. In dit geval zou dat dus max(2, 1) = 2 zijn.

Dit is alleen niet het geval als algoritmes in hybride vorm worden gebruikt: dan wordt van de twee algoritmes in hybride modus eerst de minimum score genomen. Een toelichting over hybride algoritmes staat in sectie 2.3. Zoals genoemd in Sectie 2.3, is bij een hybride systeem je systeem zo sterk als het sterkste algoritme in het systeem.

Tabel 2.2: Voorbeeld cryptografische kwetsbaarheidsscore per systeem.

Systeem		Scores gevonden algoritmes	Applicatie kwetsbaarheidsscore
Applicatie A	RSA-2048	2	2
Applicatie B	RSA-4096, AES-128, SHA2-256	2, 1, 0	2
Applicatie C	Hybride(Crystals-Kyber, ECDH), AES-128	Hybride(0,2), 1	1
Applicatie D	AES-256, SHA3-256	0, 0	0

Voorbeeld_Cryptografische_Inventaris.xlsx:

De voorbeeld inventaris bevat uitgebreidere voorbeelden. Voor Applicatie A zijn 7 verschillende algoritmes gevonden waarvan er 2 in hybride context worden gebruikt.

In de kolom *quantum kwetsbaarheid* staan de bijhorende scores. Het gevonden algoritme DES is vandaag de dag al niet meer veilig en resulteert daarom in een '!'. Dit betekent dat dit een belangrijke bevinding is, maar dat het niet relevant is voor een quantum-risico analyse.

Let op:
Onbekende algoritmes, plekken met *geen encryptie* of onderdelen met een *klassiek risico "!"* tellen niet mee voor het berekenen van de quantum risicoscore in dit voorbeelddocument.

Om een goed beeld te krijgen over het totale risico wat je loopt als organisatie heb je niet alleen de cryptografische kwetsbaarheid nodig, maar is het ook van belang dat je weet wat de impact op het betreffende IT/OT systeem zou zijn als er een quantum computer de cryptografie kan breken. Dit wordt in de volgende sectie verder toegelicht.

2.5 Impact analyse

De impact bepaalt hoe groot de gevolgen zijn voor een systeem, mocht de cryptografie gebroken worden door een aanvaller. Ga na welk type aanvallers voor uw organisatie realistisch zijn en weeg deze mee tijdens het doorlopen van de impact flowchart. Let daarbij ook op dat de hier gegeven impact op systeem niveau is, en dat het aan de organisatie zelf is om te bepalen wat de business impact is behorende bij een IT/OT systeem.

Net zoals bij het bepalen van het cryptografische kwetsbaarheid delen we de impact in op drie niveaus. Om de impact in te kunnen schatten kan de flowchart uit figuur 2.2 gebruikt worden. Mocht een specifieke applicatie niet passen in de generieke flowchart, kan de impact ingeschat worden aan de hand van de volgende interpretatie van de drie impact niveaus:

- **Impact niveau 1:** Geen dreiging waar acuut iets aan gedaan hoeft te worden. Dit kan bijvoorbeeld zijn omdat de cryptografie geen gevoelige applicatie beveiligt, omdat de dreiging pas begint over tien jaar, of omdat er geen realistische aanvaller bestaat om de dreiging uit te buiten.
- **Impact niveau 2:** In dit geval is er een bestaande dreiging van een realistische aanvaller, maar niet op zeer korte termijn. Dit is bijvoorbeeld het geval als er wel risico is op het nu onderscheppen en later ontsleutelen van gevoelige data, maar dat deze tegen die tijd niet meer relevant is. Een ander scenario is een applicatie die een hoge business impact heeft, zoals het verifiëren van een identiteit of het voorkomen van manipulatie van software updates. In deze gevallen is er pas een dreiging wanneer een quantum computer groot genoeg is, maar op dat moment is de kans ook hoog. Daarom is het essentieel om op tijd gemigreerd te zijn naar *post-quantum cryptografie*.
- **Impact niveau 3:** Het hoogste impact niveau waar acuut iets aan gedaan moet worden. Er is dan reeds een realistische aanvaller, die data kan onderscheppen om te ontsleutelen zodra ze een quantum computer ter beschikking hebben. Deze data heeft op het moment van ontsleutelen nog een significante business impact. Denk hierbij bijvoorbeeld aan staatsgeheimen, intellectuele bedrijfsgeheimen, confidentiele contracten, of bijzondere persoonsgegevens.

Harvest-now-decrypt later: impact hangt af van het doel van de cryptografie

Impact van de quantum computer raakt de confidentialiteit anders dan de authenticiteit en integriteit.

Over het algemeen geldt dat de hoogste impact ontstaat als er een kans is op het onderscheppen en ontsleutelen van data dat over een lange termijn *geheim* moet blijven en de cryptografie daarop niet berekend is.

Als de versleutelde data nu wordt onderschept en bewaard tot het moment dat deze met een quantum computer kan worden ontsleuteld, heet dit “harvest-now-decrypt-later”. Dit kan interessant zijn voor een aanvaller als data lang waardevol blijft. Een dergelijke zwakheid vereist daarom eerder actie, bijvoorbeeld:
Versleutelde data moet twintig jaar geheim blijven, wordt vandaag de dag onderschept, en een quantum computer kan dit ontsleutelen over 15 jaar: dan lopen we nu 5 jaar achter met een migratie naar post-quantum cryptografie.

Als hetzelfde mechanisme wordt gebruikt voor data waar de integriteit of authenticiteit wordt gegarandeerd met cryptografie, is de impact meestal kortlopend: authenticiteit en integriteit zijn vaak alleen van belang op het moment dat data ontvangen wordt, of zolang als een digitale identiteit geldig is. Een organisatie heeft dan meer tijd om te migreren naar post-quantum cryptografie.

Cryptografie die gebruikt wordt voor onweerlegbaarheid, bijvoorbeeld een digitale handtekening op een document die bewijst dat persoon A een huis heeft gekocht, is een speciaal geval. Meestal is de impact hierbij ook hoog, omdat deze contracten lang geldig moeten zijn. Een aanvaller met een sterke quantum computer kan een handtekening vervalsen. Dit kan eenvoudig voorkomen worden door *voor* dit moment certificaten *opnieuw* uit te geven gebruikmakende van een nieuw PQC algoritme, maar dat vereist wel dat er een overzicht is welke certificaten gemaakt zijn met het oude algoritme.

De resulterende impactscore is een momentopname: het is afhankelijk van de gevoeligheid van data in de applicatie, en van de huidige inschatting hoe lang het nog duurt tot de quantum computer sterk genoeg is voor het kraken van cryptografie. Deze veranderen allebei met de tijd.

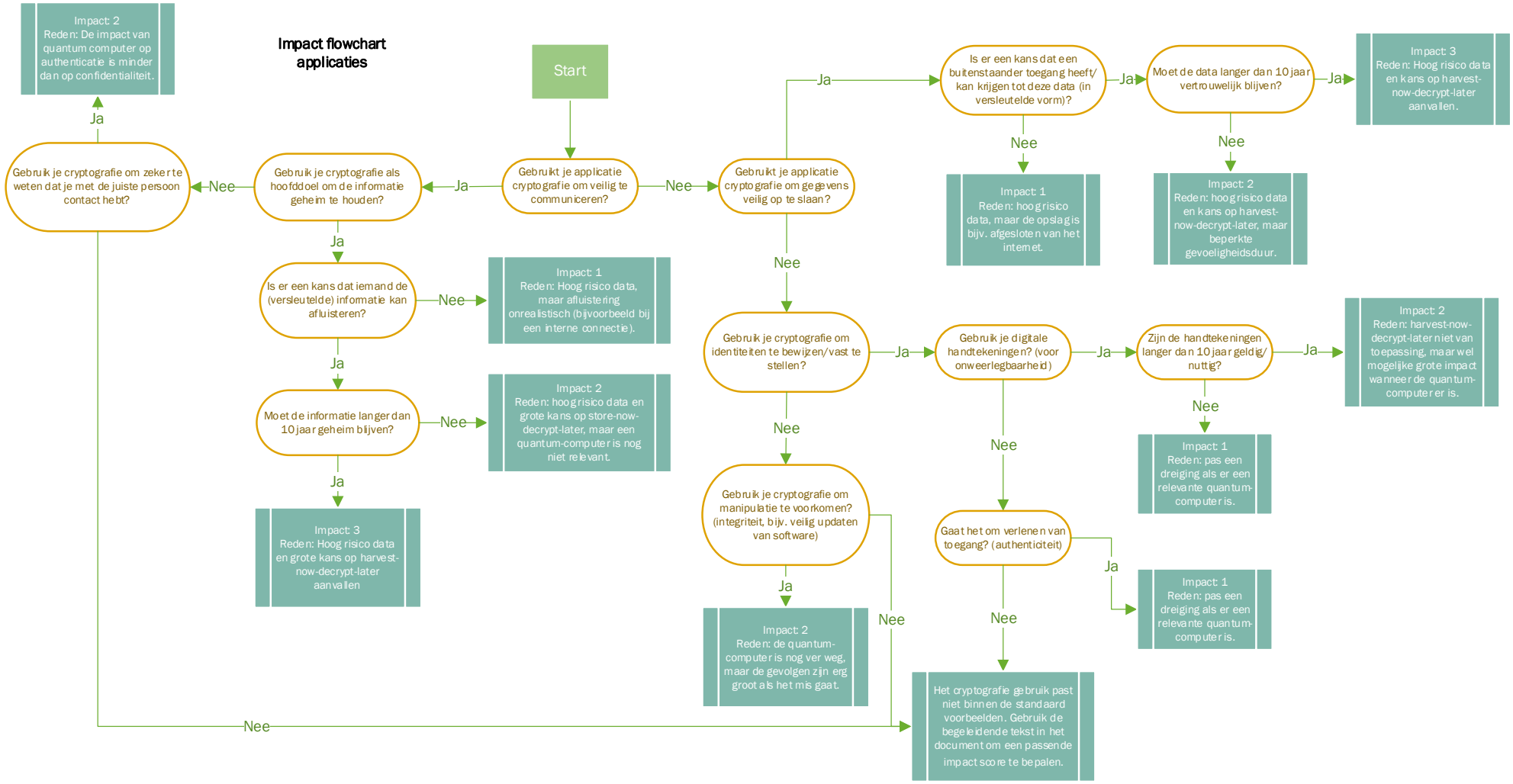
Tot slot moet benadrukt worden dat de impactscore kan veranderen als er aanpassingen gedaan worden aan het systeem. Zo zal bijvoorbeeld een data opslag van zeer geheime informatie geen hoge impactscore hebben als deze op geen enkele manier benaderd kan worden door een aanvaller. Echter, zodra deze wel verstuurd zou worden over bijvoorbeeld een internet toepassing, dan is de impact direct veel groter. Het is daarom aan te raden om met behulp van dit document, of doorlopend, de impact opnieuw vast te stellen als een wijziging aan het systeem doorgevoerd wordt.

Informatie beveiliging versus veiligheid

Meestal wordt cryptografie gebruikt voor beveiligingsdoeleinden, en de flowchart en toelichting in dit document focust daarom op beveiliging. In sommige niche toepassingen, zoals industriële systemen (OT), dient cryptografie ook een *veiligheid* aspect.

Neem bijvoorbeeld de digitale handtekening op de firmware van SCADA systemen. De handtekening voorkomt manipulatie van de firmware. Manipulatie van firmware zou kunnen leiden tot veiligheidsrisico's.

Indien er sprake is van OT systemen, is de impact op veiligheid ook een factor die moet worden meegenomen in de impact score.



Figuur 2.2: Impact flowchart

2.6 Migratie-moeite

Om een volledige quantum risicoanalyse uit te voeren, is het van belang om een analyse te maken van de benodigde kosten, tijd, en moeite om over te schakelen naar PQC. Om het simpel te houden is er voor gekozen om hier, net als bij de impact en de cryptografie, een score te geven met 3 verschillende niveaus. Deze zijn als volgt:

1. Migratiescore 1 betekent dat er geen grote problemen worden verwacht. De verwachting is dat de tijd om volledig over te stappen op PQC ongeveer 2 jaar is.
2. Migratiescore 2 betekent dat de migratie niet triviaal is, maar ook niet heel moeilijk. De verwachting is dat de tijd om volledig over te stappen naar PQC tussen de 5-8 jaar zal zijn.
3. Migratiescore 3 betekent dat de migratie erg lastig zal zijn. Een systeem heeft bijvoorbeeld veel afhankelijkheden, er is een gebrek aan prioriteit of personeel, is moeilijk fysiek bereikbaar, of er spelen andere potentieel vertragende factoren. De verwachting is dat het langer dan 8 jaar duurt om volledig over te stappen naar PQC.

De migratie-moeite is een metriek die afhankelijk is van de complexiteit van de overstap van klassieke cryptografie, zoals RSA en ECC, naar PQC, uitgedrukt in termen van **tijd en kosten**. Het is erg organisatie afhankelijk en hangt af van vele factoren, daarom is er hier geen flowchart voor te maken. Vraag applicatiebeheerders of andere interne experts om input te leveren voor het bepalen van het juiste niveau. De volgende informatie en de voorbeelden kunnen helpen bij het bepalen van deze score.
Factoren die de migratie-moeite beïnvloeden zijn:

- **Volwassenheid beheerorganisatie**. Een organisatie die zijn life cycle management goed op orde heeft, heeft vaak al goede processen rondom asset management (inclusief certificaat management). In dat geval is het vinden en migreren van de cryptografie eenvoudiger omdat gebouwd kan worden op bestaande processen.
- **Afhankelijkheid van standaardisatie en wetgeving**. Het aanpassen van standaarden of wetgeving naar post-quantum cryptografie kan een langdurig proces zijn, waar u mogelijk weinig tot geen invloed op heeft. Neem bijvoorbeeld de EMV-standaarden die bepalen welke cryptografie wordt gebruikt in bankpassen. Andersom kan wetgeving, zoals de recente Amerikaanse wetgeving[3], ook een versnellende factor zijn.
- **Externe afhankelijkheden**. Ook dit kan een zowel positieve als negatieve impact hebben op de migratietijd en -inspanning. Is de software die de cryptografie gebruikt actief in ontwikkeling en wordt er al gewerkt aan PQC? Of bevindt de software zich al in de "end of life"-fase en verwachten we geen updates meer? Bestaat de leverancier van de software nog, en zo ja, is deze gemotiveerd om een quantum veilige versie te leveren? De noodzaak tot “backwards compatibility” met andere systemen die niet geüpdatet zijn of gaan worden kan ook een complicerende factor zijn.
- **Hardware afhankelijkheid.** Als de cryptografische sleutels worden gecreëerd of beheerd op bijvoorbeeld een HSM, moet deze HSM de nieuwe algoritmes ondersteunen voordat de applicatie kan migreren. Als de toepassing hardware acceleratie gebruikt voor het snel versleutelen van grote hoeveelheden gegevens, moet worden beoordeeld of deze hardware ook geschikt is voor de nieuwe

[3] Quantum Computing Cybersecurity Preparedness Act, 2022 which requires action on post-quantum migration such as an inventory of vulnerable systems within 6 months for American Federal Systems.

algoritmes en of het snelheidsverschil acceptabel is. Voor sommige OT systemen zijn er maar beperkte hardware capaciteiten en software updates mogelijk. Deze zijn daarnaast soms lastig digitaal of fysiek te benaderen.

- **Beperkingen in bandbreedte, opslag, snelheid of ondersteunde operaties**. Kan het systeem PQC aan? PQC-algoritmes hebben andere eigenschappen dan de huidige cryptografie, wat mogelijk andere vereisten met zich meebrengt: ze kunnen bijvoorbeeld grotere sleutels nodig hebben (meer opslag vereisen) of grotere handtekeningen/ciphertexts produceren (meer bandbreedte vereisen), of intensiever zijn in termen van berekeningen (CPU/snelheid). Systemen die hier mogelijk last van ondervinden zijn onder andere smartcards (beperkte opslag- en rekenkracht), IoT- en OT-apparatuur, of juist systemen die veel cryptografische bewerkingen uitvoeren (zoals een corporate netwerk-endpoint die TLS-verbindingen verbreekt en opnieuw opzet). Als dit moet worden onderzocht, kan dit een vertragende factor zijn, vooral als het resulteert in niet alleen het updaten van een algoritme, maar ook in een vernieuwing van de cryptografische architectuur of hardware.
- **Zelfgeschreven code**. Is de applicatie intern ontwikkeld? Is de expertise in huis om dit zelf te migreren? Bij positief antwoord op dit laatste kan dit een versnellende factor zijn, of bij een tegengesteld antwoord juist een uitdaging.

Voorbeelden:

a) Applicatie A maakt momenteel gebruik van RSA en ECDH. Deze applicatie is intern ontwikkeld en maakt gebruik van de populaire library: *Bouncy Castle* voor de cryptografie. *Bouncy Castle* ondersteund al verschillende PQC-algoritmes. Bovendien zijn de programmeurs bekwaam genoeg om tests uit te voeren met de nieuwe algoritmes. Gezien deze omstandigheden krijgt Applicatie A een migratie-moeite score van 1.

b) Systeem B is een high-end router/network-endpoint die TLS-verbindingen beëindigt, packetinspectie uitvoert en informatie hercrypt voor het interne netwerk. De router wordt nog steeds actief ondersteund, en de leverancier geeft aan dat ze onderzoek doen naar PQC-ondersteuning, maar heeft nog geen definitieve tijdslijnen vastgesteld. De reputatie van de leverancier is goed; ze hebben bijvoorbeeld snel gereageerd op de migratie van MD-5 en SHA-1 naar SHA-256. Bovendien hebben de apparaten voldoende overcapaciteit om zwaardere cryptografie te verwerken. Gezien deze omstandigheden krijgt Applicatie B een migratie-moeite score van 2.

c) Systeem C betreft de PKI van een bedrijf, waarbij een eigen interne root-CA wordt gebruikt. Zowel de root- als de intermediate-certificaten (die RSA gebruiken) worden gemaakt op HSM's. Deze HSM's voeren veel cryptografische operaties uit met betrekking tot de uitgifte van certificaten. Een deel van de cryptografie wordt bepaald door geldende standaarden, waarbij in het verleden veranderingen aan deze standaarden lang hebben geduurd. De HSM's bereiken over 2 jaar het einde van hun levensduur, en het is niet te verwachten dat deze nog firmware-ondersteuning zullen krijgen voor PQC-algoritmes. Het is wachten op nieuwe HSM's met hardware-ondersteuning voor PQC. Bovendien moeten na de migratie de root- en intermediate-certificaten opnieuw worden uitgegeven, wat een tijdrovend proces is. Gezien deze omstandigheden heeft Applicatie C een migratie-moeite score van 3.

2.7 Het bepalen van risicoscores

Na het bepalen van scores voor het cryptografisch kwetsbaarheid, de verwachte impact en de moeite van het migreren volgt een quantum risicoscore per applicatie tussen 0 en 4. Deze kan opgezocht worden in onderstaande tabel.

Tabel 2.3: Risicoscores

Kwetsbaar-heid	Impact	Migratie-moeite	Risico
0	*	*	**0**
1	1	1	**1**
1	1	2	**1**
1	1	3	**1**
1	2	1	**1**
1	2	2	**1**
1	2	3	**1**
1	3	1	**1**
1	3	2	**2**
1	3	3	**2**
2	1	1	**1**
2	1	2	**1**
2	1	3	**2**
2	2	1	**2**
2	2	2	**2**
2	2	3	**3**
2	3	1	**3**
2	3	2	**4**
2	3	3	**4**

In alle gevallen zal een cryptografische kwetsbaarheid van 0 resulteren in een risico van 0, omdat de applicatie al adequaat beschermd is.

Een risicoscore 0: Geen risico
In dit geval zijn alle quantum gevaren volledig afgedekt met adequate algoritmes.

Een risicoscore 1: Laag risico
In dit geval is er wel een risico op de langere termijn, maar er hoeft op dit moment geen prioriteit gegeven te worden aan het mitigeren van dit risico.

Een risicoscore 2: Gemiddeld risico
Er moet actie worden ondernomen, maar de huidige cryptografie is voorlopig nog veilig. Of, de migratie zal naar verwachting soepel verlopen.

Een risicoscore 3: **Hoog risico**
Bij systemen met risicoscore 3 moet op korte termijn begonnen worden aan de migratie, bijvoorbeeld omdat de migratie naar verwachting lang gaat duren of omdat de impact van een aanval op het systeem erg hoog is.

Een risicoscore 4: Acuut risico
Een risicoscore van 4 is er een acuut risico, bijvoorbeeld omdat de verwachte migratietijd in combinatie met hoelang de data veilig moet blijven groter is dan de verwachte tijd tot de quantum computer de cryptografie kan breken. In dit geval duidt het op een reële dreiging die waarschijnlijk onmiddellijk moet worden aangepakt. Bij een hoge business impact is management niveau aandacht vereist.

De risicoscore is een moment opname. Risico's kunnen verlaagd worden door migratie of andere mitigerende maatregelen. Voor meer informatie over migratie, PQC algoritmes en hybride gebruik verwijzen we naar het handboek [1].

Referenties

[1] TNO, CWI, AIVD, „Het PQC-migratie handboek, versie 2,” 2023.

[2] M. Mosca en M. Piani, „2021 Quantum Threat Timeline Report,” Global Risk Institute, 2022.

[3] FS-ISAC, „Post-Quantum Cryptography (PQC) Working Group: Risk Model Technical Paper,” FS-ISAC, Inc., 2023.

[4] C. Ma, L. Colon, J. Dera, B. Rashidi en V. Garg, „CARAF: crypto agility risk assessment framework,” *Journal of Cybersecurity,* 2021.

Bijlage A

Checklist cryptografie locaties

Onderstaande tabel is een overzicht van alle plekken waar je cryptografie verwacht. tabel a.2 bevat een lijst van systemen waar je informatie kan vinden *over* de cryptografie.

Tabel A.1: Systemen die vaak cryptografie gebruiken: systemen waar je informatie over wil verzamelen

Database systemen	In gebruik voor het opslaan van sleutels, maar ook bij de database encryptie wordt cryptografie gebruikt..
Virtualisatiesoftware	Encryptie die wordt gebruikt om de VM te beveiligen. Een voorbeeld van een systeem dat sleutels beheerd is Vsphere Native Key Provider.
Interne infrastructuur voor gebruiker naar systeem connecties	SSH (SSH sleutels), VPNs, Remote Desktop connecties, SFTP (SSH File Transfer Protocol).
Interne infrastructuur tussen systemen	Beveiliging van verbindingen tussen servers/applicaties, workstations en resources. Voorbeelden zijn netwerk schijven, sharepoint omgevingen, mobile device management, API beveiliging.
E-mail encryptie	Bijv. S/MIME, maar ook bijvoorbeeld startTLS in mailservers.
Interne infrastructuur verbinding met externe services	Verbinding tussen servers en externe API's, servers. Deze gebruiken vrijwel altijd cryptografie voor authenticatie en versleuteling.
Interne infrastructuur verbinding naar externe gebruikers	Server-client verbindingen (bijv. TLS op een website).
Handtekeningen op software	Ontwikkelde en gedistribueerde applicaties bevatten vaak een handtekening om authenticiteit te bewijzen en manipulatie te voorkomen.
Interne/externe PKI (public key infrastructure)	De PKI (het systeem dat certificaten regelt). De cryptografie die hier wordt gebruikt is vaak extra gevoelig (vooral private keys van root- en intermediate CA's), en deze sleutels hebben soms lange geldigheid. Kan ook een goede bron zijn over applicatiesleutels.
Hardware Security Modules	Encryptiesleutels die de inhoud van de HSM beschermen (masterkeys). Kan ook een goede bron zijn over applicatiesleutels .
Authenticatie oplossingen	Active directory (AD), two factor systemen (2FA), LDAP (Lightweight Directory Access Protocol).
Fysieke toegangsbeveiliging	Poortjes, pasjes, etc.
Cryptografie in applicaties	De meeste applicaties gebruiken wel eens cryptografie. Denk aan wachtwoordhashing, database encryptie, versleutelde communicatie met de gebruiker, authenticatie.
IOT (Internet of Things)	Thermostaten, camera's (CCTV systeem), lampen, sloten, toegangssystemen (deuren en poortjes).

ICS (Industrial Control System)	SCADA systemen.
Backupsystemen	Zowel de back-ups van sleutels als de cryptografie die de back-ups zelf beschermt.
PDF/Documenten ondertekenen	Bijvoorbeeld voor juridische doeleinden, denk aan contracten.
Security producten	Bijvoorbeeld: handtekeningen gebruikt in virusscanners, cryptografie toegepast in inbraak preventie/detectie systemen (IDS en IPS).
Netwerk Beveiliging	Bijvoorbeeld WPA2 (wifi).
Software updates	Bijvoorbeeld hash checks voor automatische updates.

Tabel A.2: Bronnen met informatie over systemen/cryptografische details

Sleutelmanagement software	Keyvault, azure managed HSM, AWS KMS, AWS secrets manager, cred hub. Bij sommige producten, bijvoorbeeld in de cloud, kan een cloud admin een globaal overzicht opvragen van sleutels die in gebruik zijn.
HSM software/crypto teams/PKI teams/PKI management software	Certificaten zijn een goed startpunt welke applicatie welke crypto gebruikt, vooral voor asymmetrische cryptografie. Ook kan het zijn dat er logs zijn welke sleutels zijn uitgegeven op HSMs, of hebben teams die PKI/HSMs beheren overzichten.
CMDB (Configuratie Management Database)	Bijvoorbeeld voor kubernetes (kubernetes config. files). Configuraties voor VPNs, routers etc. worden wellicht ook centraal opgeslagen/zijn opvraagbaar en bevatten informatie over algoritmes en sleutels.
Development streets (OTAP in NL), CI/CD pipeline software	Hulpmiddelen voor het ontdekken van kwetsbaarheden en het beoordelen van de kwaliteit van code kunnen ook worden gebruikt om het gebruik van cryptografie te detecteren. Voorbeelden hiervan zijn SonarQube en GitLab-quality-plugins.
IT/security Architectuur overzichten	Architectuurplaten kunnen securityontwerpen bevatten met cryptografische informatie, vooral voor geïsoleerde systemen die niet toegankelijk zijn voor scanners of die in een semi-offline omgeving draaien, zoals toegangssystemen voor gebouwen.
Netwerk scanners	Portscanners zijn in staat om de gebruikte protocollen te identificeren en bieden vaak mogelijkheden om cryptografische informatie te onthullen, zoals bijvoorbeeld nmap met de optie ssl-enum-ciphers. Perimeter-scanners, zoals Qualys SSL Test, geven uitgebreide informatie over openstaande TLS-verbindingen naar het internet, zoals bijvoorbeeld voor een website met HTTPS.
Kwetsbaarheid scanners	Kwetsbaarheidsscanners zijn in staat om verouderde en onveilige cryptografie te detecteren. Sommige scanners bieden de mogelijkheid om aangepaste beleidsregels te gebruiken om alle vormen van cryptografie te identificeren. Er zijn zelfs scanners met scanprofielen die informatie kunnen verzamelen over TLS-ciphersuites. Het is belangrijk om niet alleen te denken aan scanners die het netwerk bekijken, maar ook aan scanners die worden ingezet op servers en werkplekken, evenals scanners voor 'code repositories' zoals Git en Nexus.
Incident Response Plan	Backup- en herstelplannen kunnen mogelijk inzicht verschaffen in de onderlinge afhankelijkheden tussen systemen, en in sommige gevallen zelfs in de afhankelijkheden van sleutels.

ITSM (IT Service Management)	Meestal zullen de IT Service Management (ITSM) systemen geen informatie over de cryptografische sleutels zelf bevatten. Ze bevatten echter vaak waardevolle informatie over het doel of gevoeligheid van IT componenten, zoals een BIV/CIA (Betrouwbaarheid, Integriteit, Vertrouwelijkheid) score.
ISMS systemen	Een Information Security Management Systeem wordt gebruikt om veiligheidsrisico's te identificeren en heersen. Het quantum risico kan daar deel van uitmaken.
(D)PIA (privacy impact assessment)	Privacy assessments hebben mogelijk informatie over hoe gevoelig data/een applicatie is en hoelang data gevoelig blijft, informatie die nodig is om risico's in te schatten. Omdat cryptografie een mitigerende maatregel kan zijn om privacy risico te verlagen, bevat het soms ook informatie over cryptografie.
Security assessments/pentest rapporten	Pentests vinden regelmatig kwetsbaarheden die te maken hebben met verouderde cryptografische algoritmes, of verkeerd geconfigureerde cryptografie.
Policy/beleid/ISO-certificering	Is er beleid waar sleutels opgeslagen moeten worden? Is er beleid waar cryptografie gebruik geregistreerd moet worden?

Bijlage B
Checklist cryptografische inventaris

Er is niet één inventarisformaat dat geschikt is voor iedereen. Wat je wilt registreren hangt af van het doel en de hoeveelheid manueel werk. Als het doel alleen het inschatten van een migratierisico is, volstaat met de informatie onder “basis”. Het kan wellicht waardevol zijn om verder te denken dan het quantum risico: het vraagt relatief weinig extra inspanning om aanvullende informatie te verzamelen, waardoor de inventaris breder ingezet worden. Dit verhoogt wellicht het draagvlak voor de inventarisatie.

Andere inventaris doeleinden

Extra doelen kunnen zijn:

- *Crypto-agility.* Voorbereiding op andere cryptografische kwetsbaarheden. Er zijn tal van voorbeelden geweest in de afgelopen jaren waarbij algoritmes niet meer veilig bleken, of sleutellengtes onvoldoende. Denk aan MD5, SHA-1, DES, RC4, RSA-1024. Een complete inventaris kan helpen om sneller te kunnen reageren als dit in de toekomst weer plaats vindt. Hiervoor is wel een inventaris nodig die zich niet alleen focust op de algoritmes die geraakt worden door een quantum computer.
- *Bron bij beveiligingsincidenten*. Stel een sleutel komt op straat (of op het internet), of een server die sleutels bevat wordt gehackt. Als je een overzicht hebt waar instaat waar een sleutel gebruikt wordt kan je die snel vervangen, én weet je zeker dat je de impact volledig hebt beperkt. Je kan ook weloverwogen keuzes maken over welke klanten je moet waarschuwen, welke systemen je moet isoleren, en over welke data je een privacy melding moet doen bij de autoriteiten. Hiervoor is wel informatie nodig over niet alleen het cryptografische algoritme, maar ook de sleutel en eventueel het bijbehorende certificaat.
  Verlopen certificaten zijn regelmatig de oorzaak van beschikbaarheidsincidenten, waardoor bijvoorbeeld een website niet meer bereikbaar is. Een goed overzicht helpt dit sneller te verhelpen. Hiervoor is wel informatie nodig over niet alleen het cryptografische algoritme, maar ook de sleutel en het bijbehorende certificaat.
- *Voldoen aan verplichtingen.* Sommige certificeringen vereisen een goed overzicht van sleutels en cryptografie (bijvoorbeeld PCI-DSS[4] of ABDO[5]).

Zie voor extra informatie die nodig is voor deze doeleinden.

Automatisering

Afhankelijk van de grootte van je IT landschap, wil je het vullen (en updaten) van een inventaris (deels) automatiseren. Dit kan voordelen hebben: je kan makkelijker je inventaris periodiek updaten, en het is minder foutgevoelig. Een uitdaging is wel het goed koppelen van informatie, het voorkomen van dubbele resultaten en het voorkomen van foute bevindingen. Een combinatie is ook mogelijk: een automatische detectie van de cryptografie, met de risico informatie handmatig ingevuld.

[4] Official PCI Security Standards Council Site - Document
[5] ABDO 2019 | Beleidsnota | Defensie.nl

Dit betekent voor je inventaris dat je in ieder geval informatie wil toevoegen over de bron van de informatie (welke scanner) en het tijdstip van de scan (Algoritme A gevonden op 1 april, niet meer in gebruik op 1 mei). Als je een deel van de risico inschatting wilt automatiseren i.p.v. handmatig bepalen, wil je bijpassende informatie registreren, zie hiervoor tabel b.4

Basis informatie in inventaris:

Tabel B.1: Basis informatie over algoritmes.

	Informatie op algoritme niveau
Unieke identifier applicatie/systeem	Om de gevonden algoritmes te koppelen aan de applicatie (in ruime zin, dit kan ook een systeem zijn).
Algoritme	Bijvoorbeeld RSA, SHA2
Sleutellengte of hashfunctie output lengte	Bijvoorbeeld RSA-3072, SHA3-256, AES-128
Doeleinde algoritme	Sleuteluitwisseling, digitale handtekening (authenticiteit), digitale handtekening (onweerlegbaarheid), confidentialiteit, bericht integriteit en authenticiteit
Levensduur sleutel	Hoe lang wordt een sleutel gebruikt: Sessie, 1 jaar, verloopt niet
Quantum kwetsbaarheid score	Score 1,2 of 3, zie sectie 2.4.1.

Tabel B.2: Basis informatie over systemen.

	Informatie op applicatie niveau
Unieke identifier applicatie	Om de gevonden algoritmes te koppelen aan de applicatie (in ruime zin, dit kan ook een systeem zijn).
Applicatie quantum kwetsbaarheid score	Het maximum van de quantum kwetsbaarheidsscore van zijn cryptografische componenten. Bij hybride gebruik (bijvoorbeeld ECDH+Kyber) wordt van deze scores eerst het minimum gepakt, zie sectie 0.
Impact score	Dit kan manueel worden bepaald, bijvoorbeeld door middel van de flowchart, of automatisch (maar dan is er data nodig zoals gesuggereerd in de tweede tabel hierna). Zie sectie 2.5.
Migratie-moeite	Dit kan manueel worden bepaald, bijvoorbeeld door middel van de informatie in dit document. Automatisch kan in theorie, maar is subjectiever dan risico en impact. Zie sectie 2.6.
Quantum risico	Met de 3 scores (kwetsbaarheid, impact en migratie) wordt door middel van een tabel (automatisch) het uiteindelijke risico berekend. Zie sectie 2.7.

Extra informatie indien inventaris wordt gebruikt voor andere doeleinden:

Tabel B.3: Extra informatie voor een inventaris.

Huidig risico	Is dit algoritme op dit moment nog veilig genoeg? Handig voor bredere cryptografische security assessments
Relatie met andere cryptografische componenten	Algoritmes staan meestal niet op zichzelf, maar kunnen afhankelijk van elkaar zijn. Een key exchange algoritme, zoals RSA of ECDH, wordt gebruikt om een sleutel uit te wisselen. Deze wordt vervolgens door een ander algoritme gebruikt, bijvoorbeeld AES. Als het ECDH algoritme niet meer veilig is, is daardoor ook de sleutel die in AES gebruikt wordt niet meer veilig. Asymmetrische sleutels worden vaak in combinatie met een certificaat gebruikt. Als sleutels alleen in een HSM of alleen in versleutelde vorm gebruikt worden, zijn deze afhankelijk van een HSM sleutel. Handig om te registreren voor incident response en bij audits.
Sleutelnaam	De meeste algoritmes gebruiken een sleutel. De sleutel is het belangrijkste component dat veilig gehouden moet worden. Registratie van sleutelnamen helpt om deze uit elkaar te houden. Handig voor bij audits, het eigen sleutel-management, en bij incident response.
Locatie sleutel	Waar is de sleutel opgeslagen. Onbeschermd in een configuratie? In een beveiligde omgeving zoals credhub of keyvault? In een HSM? Handig voor security assessments, bij audits, en bij incident response.

Extra informatie indien automatisering wordt gebruikt voor inventaris:

Tabel B.4: Extra informatie bij automatisering van inventaris.

Bron	Waar komt de informatie vandaan, welke scanner/agent? Voor automatische vulling van het cryptografie overzicht.
Scan tijdstip	Wanneer is de informatie gevonden? Voor automatische vulling van het cryptografie overzicht, en het traceren van de migratie gedurende de tijd.
Confidentialiteitsduur	Hoe lang moet de beschermde data confidentieel blijven? Let op, niet *bewaard* blijven, maar confidentieel blijven. Voor automatische berekening van de impact score.
Onweerlegbaarheidsduur	Hoe lang moet een digitale handtekening voor onweerlegbaarheid geldig blijven? Voor automatische berekening van de impact score.
Authenticiteit/ integriteitsduur	Hoe lang moeten de integriteit en authenticiteit verifieerbaar blijven? Voor automatische berekening van de impact score.
Migratie kenmerken	Afhankelijk van derde partijen, wetgeving, gebrek aan kennis, beperkte toegang tot hardware, legacy-systeem, geen geschikt vervangend PQC algoritme, etc.

Bijlage C

Kwetsbaarheidsscores voor veelvoorkomende algoritmes

Tabel C.5: Quantum kwetsbaarheidsscore voor veelvoorkomende algoritmes.

Algoritme	Sleutel-lengte	Hash-output	Quantum Kwetsbaarheidsscore	Klassieke security zorgen
RSA	Niet relevant	N/A	2	
ElGamal	Niet relevant	N/A	2	
Paillier	Niet relevant	N/A	2	
ECDH	Niet relevant	N/A	2	
ECDSA	Niet relevant	N/A	2	
EdDSA	Niet relevant	N/A	2	
ECIES	Niet relevant	N/A	2	
CRYSTALS-Kyber/ML-KEM	Niet relevant	N/A	0	
CRYSTALS-Dilithium/ML-DSS	Niet relevant	N/A	0	
XMSS	Niet relevant	N/A	0	
LMS	Niet relevant	N/A	0	
HSS	Niet relevant	N/A	0	
FrodoKEM	Niet relevant	N/A	0	
Falcon	Niet relevant	N/A	0	
SPHINCS+	Niet relevant	N/A	0	
Classic McEliece	Niet relevant	N/A	0	
AES	128	N/A	1	
AES	192	N/A	0	
AES	256	N/A	0	
DES	56	N/A	-	!
3DES	168	N/A	-	!
Camellia	128	N/A	1	
Camellia	192	N/A	0	
Camellia	256	N/A	0	
Blowfish	variabel	N/A	1	

Twofish	128	N/A	1	
Twofish	192	N/A	0	
Twofish	256	N/A	0	
IDEA	128	N/A	1	
RC5	variabel	N/A	1	
ChaCha20	256	N/A	0	
RC4	variabel	N/A	-	!
Trivium	80	N/A	-	!
Salsa20	128	N/A	1	
Salsa20	256	N/A	0	
A5/1	64	N/A	-	!
A5/2	64	N/A	-	!
MD5	Niet relevant	N/A	-	!
SHA-1	N/A	Niet relevant	1	!
SHA-2	N/A	224	1	
SHA-2	N/A	256 - 512	0	
SHA-3	N/A	224	1	
SHA-3	N/A	256 - 512	0	
Whirlpool	N/A	512	0	
BLAKE2	N/A	224	1	
BLAKE2	N/A	256 - 512	0	
BLAKE3	N/A	224	1	
BLAKE3	N/A	256 - 512	0	
PBKDF2	N/A	N/A	0	
HKDF	N/A	N/A	0	
Argon2id	N/A	N/A	0	
scrypt	N/A	variabel	0	
bcrypt	N/A	192	0	

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl

TNO innovation for life