Alle nieuws

Cryptografische veerkracht bouwen: hoe managers de PQC-transitie kunnen aanjagen

3 months ago

Deze blog is geschreven door de deelnemers van het PQC Benchmarking-project, afkomstig van TNO, Achmea, Belastingdienst, ABN Amro en ING..

Wat is er aan de hand?

Herinner je je laatste grote Windows-migratie nog? De overgang naar IPv6? De migratie naar Post-Quantum Cryptografie is minstens zo ingrijpend, en urgenter! Waarom? Omdat een quantumcomputer met voldoende capaciteit de meeste van je beveiligingsmaatregelen kwetsbaar en ontoereikend maakt.

Waarom is dit belangrijk?

• Quantumcomputers bestaan al. Over een aantal jaren zullen ze krachtig genoeg zijn om veelgebruikte cryptografische algoritmen te kraken.
• De quantumdreiging raakt de kern van je beveiliging: cryptografie. Je loopt mogelijk nu al risico, vooral voor data die buiten je organisatie reist, vanwege “harvest now, decrypt later” aanvallen.
• Bijna alle digitale toepassingen gebruiken cryptografie voor vertrouwelijkheid, integriteit, authenticatie en authenticiteit.
• De migratie naar een veilige situatie vereist aanpassingen in een aanzienlijk deel van je IT.
• Veel van de cryptografische algoritmen die je organisatie gebruikt, moeten worden vervangen door veilige alternatieven: de zogenaamde “Post-Quantum Cryptografie”-algoritmen.
• Deze veranderingen zijn niet triviaal: de alternatieven zijn anders en kunnen prestaties beïnvloeden. Soms zijn architectuur aanpassingen nodig.
• Cryptografische wendbaarheid (“crypto agility”) vermindert de migratie-inspanningen en verhoogt de robuustheid van je organisatie tegen deze en andere cryptografische dreigingen.

Vanwege de impact kun je deze dreiging niet negeren. **Op tijd beginnen verlaagt toekomstige kosten en risico's.** Het bereiken van cryptografische wendbaarheid en vroegtijdig starten met de migratie is een **strategische keuze.**

> "Haast je als je nog tijd hebt, zodat je tijd hebt als er haast is"
>
> — Petra Wevers, PQC expert, Belastingdienst

De kennis over PQC is nog beperkt, en er is weinig ervaring met de migratie er naar toe, wat het lastig maakt om de impact van de benodigde inspanningen goed in te schatten. De PCSI doet ervaring op om dit te verbeteren: door gezamenlijk proof of concepts migraties uit te voeren op echte systemen bij de deelnemende partners. Met het doel om kennis en ervaring op te doen en te verspreiden.

Als we slechts één les uit dit project mogen trekken, is het **dat managementsupport de migratie maakt of breekt**. In deze blog willen we de cruciale rol van managers in deze transitie benadrukken.

Onze adviezen aan managers:

1. Faciliteer interne initiatieven,
2. Investeer in leveranciersmanagement,
3. Stimuleer samenwerking.

Word de quantumheld!

Moedig initiatieven aan binnen jouw team

In onze ervaring is het niet moeilijk om engineers, architecten of cryptografie-experts te vinden die aan dit onderwerp willen werken; het is moeilijk om ondersteuning voor hen te vinden om het daadwerkelijk te doen. Kennis opbouwen, proof of concepts uitvoeren, samenwerken, bestaande kennis beoordelen — niets daarvan gebeurt zonder *tijd* en *ondersteuning* vanuit het management. *Tijd* om het werk te doen, kennis op te doen, de huidige situatie te beoordelen en samenwerkingen te starten. *Ondersteuning* van een manager die het belang inziet van investeren in kennis over dit onderwerp, en het werk en de oplossingen binnen zijn/haar netwerk uitdraagt.

> “Managementsupport is cruciaal om PQC-projecten in deze vroege fase

> prioriteit te geven boven andere bedrijfsbehoeften”
>
> — Louiza Papachristodoulou, PQC expert, ASML

Het vinden van use cases om te migreren was lastig. Leveranciers waren nog niet klaar of de teams hadden geen tijd. Hier maakte managementsupport een groot verschil. Hoewel alle deelnemers toestemming hadden om aan dit project te werken, slaagden alleen degenen waar de manager verder keek en ruimte creëerde om intern echte tests te doen. Managementsupport was een sleutel tot succes. Daarnaast zorgt een manager die het team aanmoedigt, de samenwerking openlijk ondersteunt en successen viert voor positieve motivatie.

> “Bewustwording creëren over PQC was makkelijker dan praktische ervaring opdoen. We hebben binnen Achmea een team van deskundigen opgeleid dat nu onze PQC-migratie aanstuurt. Eigenaarschap nemen over PQC is essentieel voor ons succes.”
>
> — Tom Huitema & Rob Stübener, innovatieteam, Achmea

Het is verleidelijk om (delen van) de migratie uit te besteden. Wij hebben hiermee geëxperimenteerd. Onze ervaringen leerden ons dat uitbesteding (in dit geval van code migratie) aanzienlijke nadelen heeft. De overhead van delegatie was hoog, wat mogelijke besparingen tenietdeed. Bovendien wordt ervaring voornamelijk opgedaan bij de externe partij. Zelf migraties uitvoeren, vooral vroege proof of concepts, levert

interne ervaring op die latere migraties versnelt. Het intern uitvoeren van deze acties brengt ook bedrijfsspecifieke knelpunten of oplossingen aan het licht.

Leveranciers – levenscyclusbeheer

Zoals bij veel grote organisaties zijn de partners in dit project afhankelijk van leveranciersproducten voor een groot deel van hun IT. Cryptografische wendbaarheid is daardoor sterk verweven met die van onze leveranciers. Onze moeizame zoektocht naar leveranciers die al PQC kunnen leveren, toonde het belang aan van proactieve beoordeling van leveranciersgereedheid en nauwe samenwerking.

> “Vroege en duidelijke communicatie in leveranciersrelaties is essentieel voor cryptografische wendbaarheid.”
>
> — Gamze Tillem, ING

Een manier om tijdige levering van nieuwe algoritmen te waarborgen, is het implementeren van beleid. Regelgeving en vakgebied standaarden helpen organisaties om duidelijke verwachtingen te stellen en leveranciers te dwingen hun aanbod proactief bij te werken. Naast internationale standaarden en raamwerken helpt het opnemen van cryptografische wendbaarheid in service level agreements met leveranciers om de prioriteiten van je organisatie tijdig te implementeren.

> “Een probleem dat we tegenkwamen, was dat leveranciers een andere interpretatie hadden van ‘PQC-ready’ of ‘crypto-agile’ dan wij. Ondanks goede ondersteuning vanuit leveranciers, voldeden de oplossingen in meerdere gevallen niet aan het volwassenheidsniveau dat wij vereisten”
>
> — Gamze Tillem, Security Architect at ING

Effectieve communicatie met leveranciers is cruciaal om prioriteiten en tijdlijnen op elkaar af te stemmen. Leveranciers die een brede klantenkring bedienen vermijden mogelijk maatwerk, wat kan leiden tot vertragingen van je

migratieplan. Om dit te voorkomen zijn afstemming tussen leveranciersmanagement en je security-experts, duidelijke communicatie over prioriteiten en proactief verwachtingsmanagement essentieel voor het behalen van cryptografische wendbaarheidsdoelen. Zie onze blog over leveranciersmanagement voor meer informatie.

Goede samenwerkingen

Vanuit samenwerkingsperspectief lijkt dit PCSI-project niets bijzonders: gewoon een groep cryptografie- en technische experts van zes organisaties die samenwerken aan een PQC-benchmarkingproject. Duidelijke spelregels voor structuur en een ‘staged innovation approach’ om grenzen en deadlines te stellen. Klinkt als een doorsnee werkdag, toch?

Alle deelnemers droegen bij naast hun reguliere werk. Het project was uitdagend. Omgaan met prioriteiten, koerswijzigingen en tegenslagen. Maar waarom waren alle deelnemers dan zo enthousiast en werden de teamresultaten zo goed ontvangen? Dat kwam vooral door het delen van de last en het elkaar helpen bij moeilijkheden.

Een belangrijk ingrediënt is het frisse perspectief van externe partners. Inzichten in hoe dingen werken bij andere organisaties zorgen voor een andere blik. Het helpt om problemen te omzeilen, te schakelen als iets niet werkt zoals gepland. Daarnaast: weten dat je niet de enige bent met bepaalde problemen, een aanpak proberen die elders werkte — het helpt allemaal om effectief vooruitgang te boeken. Uiteindelijk hebben we in korte tijd veel ervaring opgedaan, wat alleen niet mogelijk was geweest. Voor managers geldt: ondersteun en bevorder samenwerking met externe partners; het effent de weg naar efficiëntere en rijkere oplossingen.

> “Het was interessant om de verschillende uitdagingen van de betrokken partners te zien. Sommigen hadden behoefte aan kennis, anderen aan managementsupport en bij weer anderen lag het probleem bij de gereedheid van leveranciers. Door ervaringen te delen konden we de meeste obstakels overwinnen.”
>
> — Manon de Vries, projectleider, TNO

Hoe weet je of de samenwerking de investering waard is? Van tevoren weet je dat niet. Maar uit de ervaring van het PQC Benchmarking-project blijkt dat een energiek en divers team met gedeelde focus garant staat voor goede resultaten. Het faciliteren van specialisten en het aanmoedigen om inzichten

vanuit nieuwe invalshoeken te bekijken, brengt magie in termen van samenwerking en teamcultuur. Wat op zijn beurt zorgt voor de beste opbrengst van de investering.

Belangrijkste lessen

Als manager hoef je niet alle details te begrijpen, zolang je de urgentie voelt en de complexiteit bevat. Bied tijd en ondersteuning, en promoot de resultaten in je organisatie. Moedig je experts aan, bevorder samenwerking en focus op afhankelijkheid van leveranciers. Nu starten en samenwerken verhoogt de moraal, vermindert de benodigde inspanning en beperkt het risico.

Word een Crypto-agility Held.

Houd de andere blogs in deze serie in de gaten!
In deze reeks van vier blogs delen we zowel organisatorische als technische resultaten, vanuit vier perspectieven: *Management*, *Developers*, *IT Architecten* en *Vendoren*.

Meer weten over de PQC migratie?

Het PQC Migration Handboek (NL) is een goed startpunt.

Meer weten over de Partnership for Cyber Security Innovation? Bekijk onze over ons -pagina

---

De plaatjes in dit blog zijn gemaakt met AI, en AI heeft ondersteund in de vertaling van Engels naar Nederlands.