Alle nieuws

Building Resilience: How Managers Can Champion the PQC Transition

one month ago

This blog is written by the participants of the PQC Benchmarking project, from TNO, Achmea, Belastingdienst, ABN Amro and ING.

What is happening?

Remember your last major windows migration? The transition to IPv6? The Post Quantum Cryptography migration is at least as big, with higher urgency! Why? Because a quantum computer of sufficient capacity will render most of your security vulnerable and insufficient.

Why should you care?

- Quantum computers exist today. At some point in the near future, they will be strong enough to break many widely used cryptographic algorithms.
- The quantum threat hits your security in its core: cryptography. You might already be at risk, especially for data travelling outside your company, to an attack called “harvest now decrypt later”.
- Almost all digital applications use cryptography for confidentiality, integrity, authentication and authenticity.
- The migration to a safe situation will require changes for a substantial part of your IT.
- Many of the algorithms used by your organization will need to be replaced by safe alternatives. These are called “Post Quantum Cryptography” algorithms.

- These changes are not trivial: the alternatives are different and can impact performance. In some places it will require architectural changes.
- Crypto agility will reduce the migration efforts and increase the robustness of your company for this *and* other cryptographic threats.

Due to its impact you do not have the luxury to ignore this threat**. Starting on time will decrease costs and risk in the future.** Being crypto agile and starting the migration process early is a **strategic** decision.

> "Hurry when you still have time, so you'll have time when there is a hurry"
>
> — Petra Wevers, PQC expert, Belastingdienst

Knowledge on PQC is still low, and not a lot of experience exists yet with the migration to it, making it hard to assess the impact of the necessary migration efforts. The PCSI has been gathering experiences to remedy this: by collaboratively doing migration Proof Of Concepts on real systems at the participating partners. The goal is to spread knowledge and experience.

If we are allowed only one lesson from this project, it is that **management support makes or breaks this migration**. In this blog we want highlight the crucial role of managers in this migration.

In this project we learned a lot on what helps make this process go smoothly. Our takeaways to managers:

1. Facilitate **in-house initiatives**,
2. invest in **vendor management** and
3. Foster **collaboration**.

Be the quantum hero!

Encourage and facilitate initiatives on this topic within your teams

In our experience it has *not* been hard to find engineers, architects, or cryptographic experts that want to work on this topic: it has been hard to find *support* for them to do so. Building knowledge, doing proof of concepts, collaborating, assessing existing knowledge, none of it happens without *time* and *support* by management. *Time* to do the work, to attain knowledge, to assess your situation and start collaborations.

Support of a manager that sees the value of investing in knowledge on this topic and can sell the work and solutions in his/her network within the company.

> "Management support is crucial for prioritizing PQC projects over other business needs at this "early" stage"
>
> — Louiza Papachristodoulou, PQC expert, ASML

It is tempting to outsource (part of) the migration. We experimented with this. Our experiences have taught us that outsourcing part of the work (in this case code migration) has significant drawbacks. The overhead of delegation was quite high, negating potential savings. Additionally, any *experience* gained is done at the external party. Doing migrations yourself, especially early POCs, results in experience within the company, which can aid and quicken later migrations. Doing these actions within the organization also brings to light potential pain points or solutions that are specific for your organization, knowledge of which reduces risk for the full effort.

Vendors – life cycle management

Like many large organizations, the partners involved in this project depend on vendor products for a significant portion of their IT assets. Thus, our cryptographic agility is highly intertwined with the cryptographic agility of our vendors. Our challenges in finding vendors that can provide PQC-ready tools showed us the importance of proactive assessment of vendor readiness and a close collaboration with them.

> “Early and clear communication is key in vendor relations on cryptographic agility.”
>
> — Gamze Tillem, ING

One way of assuring timely delivery of new algorithms is implementing compliance standards. Regulations and industry frameworks help organizations set clear expectations on agility and enforce vendors to stay in line with technological advancement and proactively update their offers. Apart from the international standards and frameworks, including cryptographic agility in the service level agreements with vendors ensure timely implementation of priorities of your organization.

> “One issue we observed that vendors’ interpretations of being “PQC-ready” or “crypto agile” varied from ours. Despite the great support provided by vendors,

> in several cases, the solutions did not have the level of maturity we required”
>
> — Gamze Tillem, Security Architect at ING

Effective communication with vendors is crucial in the alignment of priorities and timelines. Vendors aiming to serve a wider customer base might avoid tailoring solutions to your specific needs, which can lead to delays in your organization’s roadmaps. To prevent such challenges, alignment between vendor management and your security experts, clear communication to vendors and proactive engagement in expectations and priorities with vendors are essential in achieving cryptographic agility goals. See our blog on vendor management for more details.

Good collaborations

From a collaboration setup, this PCSI project seems like nothing special. Just a group of cryptographic and technical experts from 6 different organizations working on a PQC-benchmarking project. Clear game rules for structure and the ‘staged innovation approach’ to set boundaries and deadlines for obtaining results. Sounds just like any other day at the office, right?

All participants were contributing next to their regular work activities. The project itself was challenging. Dealing with priorities, multiple setbacks, pivots and struggles. But then, how come all participants were so enthusiastic and the team results received so incredibly well? It mostly comes down to sharing the burden and helping each other through difficulties.

A top ingredient is the freshness of external partners’ perspectives. Insights on how things work in other organizations make you take a look from a different angle. It helps to get unstuck, to pivot when things do not work out the way it is planned. Next to that: knowing you’re not the only dealing with certain struggles, taking a chance with an approach that worked for others, it all helps in progressing effectively. In the end we gained major experience in a short time which would not have been possible on our own. For any manager, fostering and supporting collaborations with external partners paves the way to efficiently finding more enriched solutions.

Keep a look out for the other blogs in this series! In this series of four we share both organizational and technical results, from four different perspectives: Management, Vendors, Architects and Developers.

Want to know more about PQC migration?

The PQC Migration Handbook (NL) is a good starting point.

Want to know more about the Partnership for Cyber Security Innovation? Check out our About us page.

The images in this blog were created using AI