Augustinus Mohn PhD CISM
is a manager at KPMG Cyber in the Netherlands.

Jan Lugtmeijer MSc
is a cybersecurity consultant at KPMG Netherlands.

Ir. Ronald Heil MSc GICSP CISSP CISA
is a partner at KPMG Cyber in the Netherlands.

Zero Trust: beyond the hype

THE ZERO TRUST HYPE

Zero Trust is not brand new and has been around for a while. The term Zero Trust was coined in 2010 by Forrester, and the concept itself can be traced back to 2004. Recently, Zero Trust as a security framework has become increasingly popular and is being more and more hyped. Reasons for this are increasingly vast and complicated networks combined with more advanced cyber threats. An example of where we see that this hype is translating more to the norm is the endorsement of the US government of Zero Trust. Last year an executive order was released that named Zero Trust Architecture as the leading security best practice along with movement to cloud and software as a service (SaaS) adoption ([WhHo21]) .

WHAT IS THE PROBLEM THAT ZERO TRUST IS CLAIMING TO SOLVE?

Opportunities for cyber breaches have expanded exponentially over the past several years. New, more mobile working arrangements, innovative cloud technology, and increased business dealings with vendors and other third parties have created a more porous perimeter, increasing the attack surface and exposing vulnerabilities (i.e., more opportunities) for cybercriminal attacks. In the face of these developments, the traditional "cybersecurity perimeter" defense (see Figure 1) has become far less effective, enabling cyber criminals and other "bad actors" to exploit weaknesses and holes with more frequency and do far more damage. The main pitfall of this model: once you are beyond the castle walls, everything can be accessed (maybe there's another tower wall for the crown jewels, but that's it).

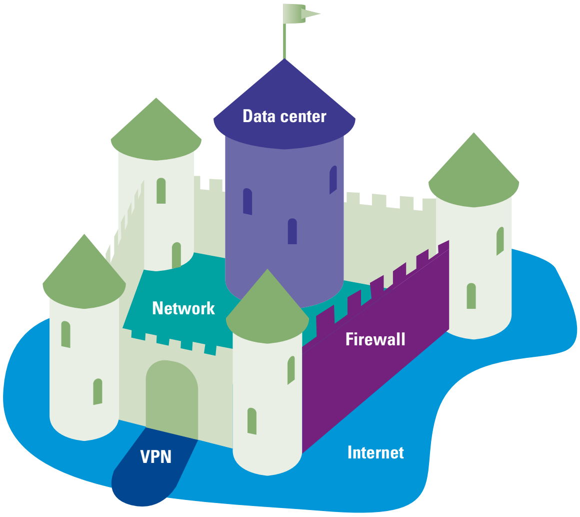

Figure 1. Outdated "castle-moat" cyber defense setup.

By 2025, global cybercrime damage is expected to reach $10.5 trillion annually ([Morg20]). And in the U.S. in 2020, the average data breach cost organizations $8.64 million ([Stat21]). Aside from a purely dollars-and-cents damage, these breaches can also have implications on worker safety as well as the environment and safety of the surrounding communities. They can also jeopardize an organization's brand and reputation, undermining its customers' trust in the reliability of the organization and the safety of their personal data. In addition, these breaches also expose the organization to litigation and regulatory penalties.

WHAT IS ZERO TRUST?

Zero Trust is a model that is often claimed to be a game changer to the old castle cyber defense setup. Instead of having one defense perimeter, access is given only on a needs-basis – after all, why should someone who needs a new sword (or a sensitive Word document) also be granted access to everything else that's in the weapons chamber – and the sleeping chambers, and the kitchen, and so forth? Zero Trust literally means "trust no-one", not even those who live in the castle (not even the king, for that matter).

Although the Zero Trust way of thinking has been around for quite some time, technology (e.g., modern cloud infrastructure and predictive analytics) has only recently caught up with the philosophy and made it feasible in practice. In more technical terms: since Zero Trust typically relies on cloud/hybrid cloud adoption, identity, and network modernization, only recently has it become conducive for organizations to realize the full potential value of Zero Trust.

With Zero Trust, you establish what is often referred to as a "perimeter-less" defense system[1] based on the principal of never trusting and always verifying individuals and devices, regardless of whether they are inside or outside of the organization. Before access to a system or app is granted, the person or device seeking access must be identified, assessed verified and authorized. And this authentication process takes place each step of the way. In other words, using the castle metaphor again, there are checkpoints installed at every door, hallway and even the treasure box wherein a specific item is contained.

With Zero Trust, whomever (or whatever) attempts to access your systems – along with the device they're using – is identified, assessed, authenticated and authorized in light of the system they are trying to access, and that

[1] Technically, a Zero Trust process is not truly perimeter-less. Zero trust does not rely on the traditional "moat" style perimeter, but instead replaces it with hundreds and thousands of smaller perimeters, each one wrapping around every user, device, connection and so on.

session is continuously monitored. And when they seek to access another system, the process is done all over again. At the same time – from a user's perspective – the process has to be set up in such a way that work becomes quick, easy and seamless.

BEYOND THE HYPE

Exaggerations and criticism aside, there are two key potential benefits of a Zero Trust approach: (1) it prevents bad actors from getting authorized and accessing your system and (2) in the event of an initial breach, your organization would be able to detect and isolate the intruding person, device or "bug" and turn off its access to the system, not allowing it to pivot or escalate the attack.

For example, one of the world's leading shipping companies was brought to a standstill by cybercriminals who installed ransomware on a local office server in the Ukraine. The virus then spread throughout the company's entire global network, causing an estimated $250 to $300 million in damages. But a Zero Trust approach, with its multiple reauthentication security and continuous session monitoring process, could have limited the damage to the Ukraine and not caused a company-wide shutdown ([Colu19]).

Similarly, in 2021, a state-owned oil company (Aramco) was the victim of a cyber-attack. The perpetrator accessed confidential data through the system of a third-party contractor with whom Aramco did business. Although its business operations weren't interrupted, the cybercriminal demanded $50 million, by threatening to sell the information to any other party for $5 million. Had Aramco been operating a Zero Trust strategy, it's unlikely its systems would have been breached ([Flas21]).

There are a host of other potential benefits to be gained by a Zero Trust approach. For example, it can:

- improve network visibility, breach detection and vulnerability management;
- break down interdepartmental silos as IT, HR, marketing, operations, compliance and others need to work together to get it right;
- reduce both capital and operational costs in the long-term;
- enable and support digital business transformation and improved business agility.

GETTING STARTED ON YOUR ZERO TRUST JOURNEY

A critical element in designing and implementing a Zero Trust architecture is understanding that it may represent a cultural change and challenge to your organization. Therefore, you will need commitment from senior management to help overcome resistance.

And while the CIO and the cybersecurity department may lead the effort, you also need the buy-in and cooperation of the entire organization – including information technology, operational technology, IOT, HR, compliance and regulatory, and sales and marketing – to get it right.

The Zero Trust security architecture must integrate with the organization's security and IT environments to enable speed and agility, improve incident response, and to support policy accuracy and the delegation of responsibilities. At the same time, the authentication and reauthentication measures cannot unduly burden the normal operations of the business, particularly in terms of wasted time.

Here are some steps to demonstrate how we would start the Zero Trust journey:

1. **Determine what you're trying to achieve.** Don't start with the solution. Determine what needs improvement and which Zero Trust components make sense. Also, keep in mind that the Zero Trust model doesn't have to be implemented all at once; it can be phased in and tailored to your organization's level of maturity.
2. **Identify and prioritize which data and assets are most valuable.** Collect as much information as possible about the current state of assets, network infrastructure and communications. Also, classify the level of "sensitivity" of each asset, for example, the customer database, source codes, confidential or proprietary information (e.g., business process), and the HR portal – which are "restricted," "highly restricted," and so on.

> "If done correctly, a Zero Trust approach doesn't just block cyber criminals and bad actors from doing things they shouldn't be able to do; it enables people to do their jobs better – with less friction and a higher degree of security."
>
> – Brad Raiford (Director, Cyber Security Services KPMG in the U.S.)

3. **Map data flows across your network.** This step is a primary reason why you need the input and cooperation of multiple departments and not just cybersecurity and IT; the Zero Trust approach impacts everyone. The data flows include:
   - North-South traffic, such as from a front-end web portal to back-end servers;
   - East-West traffic, such as purchase information to fulfillment and accounting systems within the corporate network.
4. **Group assets with similar functionalities and sensitivity levels into the same micro-segment.** This will help you determine when and where authentication and reauthentication may be needed, so you can:
   - deploy a segmentation gateway (this can be virtual or physical and will enable you to achieve control over each segment);
   - define a "least privilege" access policy to each of these assets, whereby access to services is granted based on context and the risk profile of users and devices (e.g., a public device, based in a suspicious location vs. being on company premises), and all access must be authenticated, authorized, and encrypted.
5. **Select the right technologies and services to support Zero Trust.** The cybersecurity team will be instrumental in this decision, but will certainly need input from other departments, including finance. It's critical to build in flexibility that will be needed to adapt to everchanging risks and the ability to conduct real-time monitoring and continuous assessment and anomaly detection.
   - When making the presentation to senior management or other decision makers, be prepared with a final estimate of resources needed as well as the proposed timing for implementation.

Throughout your Zero Trust journey, you should remember that Zero Trust is a principle-based approach – it is not only about technology; it's also a way of thinking that should guide your decision-making from a technological and business perspective (see Figure 2).

CONCLUSION

Zero Trust should be seen as a way of thinking that enables organizations to perform efficiently and effectively, while putting a high premium on cybersecurity. If embedded as a business project, Zero Trust can add long-lasting value – but the journey to get there requires a strong effort and leadership from the start. Meeting business needs with relevant and secure technology, and at the same time ensuring organizational buy-in, is a challenge that can best be tackled with a clear vision, a meaningful strategy, and operational involvement beyond IT. With such conditions, Zero Trust is here to stay.

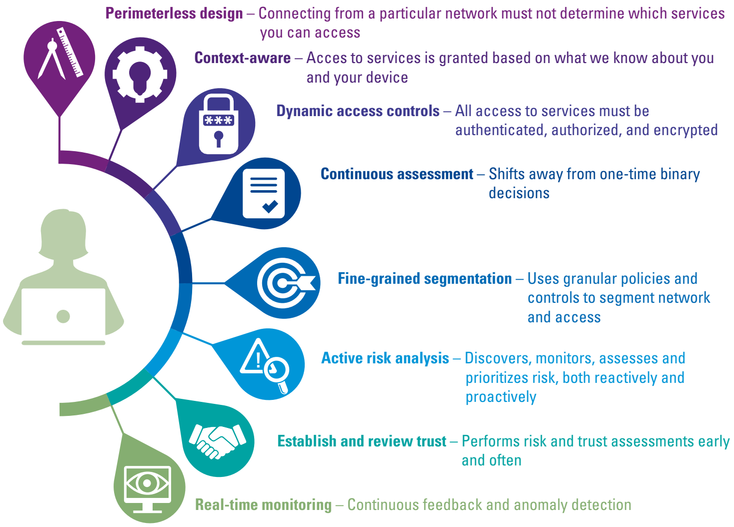
Perimeterless design – Connecting from a particular network must not determine which services you can access
Context-aware – Acces to services is granted based on what we know about you and your device
Dynamic access controls – All access to services must be authenticated, authorized, and encrypted
Continuous assessment – Shifts away from one-time binary decisions
Fine-grained segmentation – Uses granular policies and controls to segment network and access
Active risk analysis – Discovers, monitors, assesses and prioritizes risk, both reactively and proactively
Establish and review trust – Performs risk and trust assessments early and often
Real-time monitoring – Continuous feedback and anomaly detection

Figure 2. Principles of Zero Trust.

References

[Colu19] Columbus, L. (2019, August 29). Why Manufacturing Supply Chains Need Zero Trust. *Forbes.* Retrieved from: https://www.forbes.com/sites/louiscolumbus/2019/08/29/why-manufacturing-supply-chains-need-zero-trust/?sh=768e55857a73

[Flas21] Flashpoint (2021, July 23). Saudi Aramco Data Breach Highlights Risks to Oil and Gas Industry. *Flashpoint.* Retrieved from: https://www.flashpoint-intel.com/blog/saudi-aramco-data-breach-highlights-risks-to-oil-and-gas-industry/

[Lync22] Lynch, K. (2022, January 20). Biden Aims to Drive Zero-Trust Architecture Nationwide. *Mimecast.* Retrieved from: https://www.mimecast.com/blog/biden-aims-to-drive-zero-trust-architecture-nationwide/

[Morg20] Morgan, S. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine.* Retrieved from: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

[OBM22] Executive Office of the President – Office of Management and Budget (2022). Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[Stat21] Statista (2021). Average organizational cost to a business in the United States after a data breach from 2006 to 2020. Retrieved from: https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach

[WhHo21] The White House (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. Retrieved from: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

About the authors

Augustinus Mohn PhD CISM is a manager at KPMG Cyber in the Netherlands. He obtained his PhD in security studies at the University of Aberdeen in 2014 and is currently supporting the World Economic Forum with developing a global framework for Digital Trust.

Jan Lugtmeijer MSc is a cybersecurity consultant at KPMG Netherlands, who studied Information Sciences. He joined KPMG in 2020 as a trainee in the IT Assurance traineeship and has since worked on projects related to data analytics, cyber maturity, IT assurance and IT asset development.

Ir. Ronald Heil MSc GICSP CISSP CISA is a partner at KPMG Cyber, The Netherlands, leading the technical cybersecurity services. In addition, Ronald is the global service delivery lead for Security Testing, global lead for Cyber in the ENR sector and senior global SME for the industrial security services.