Cybersecurity for mission-critical communications

White Paper

While most cyber-attacks aim to achieve financial gain, the consequences of a successful attack on a mission-critical communications network can be far more damaging, even life threatening.

New, advanced services are being enabled by IP-based broadband networks and made available to public safety and other mission-critical users. The openness of such networks increases the risks with regards to the cyber-threat, calling for the right security designs, safeguards and continuous pro-active security operations.

Contents

1. Executive Summary

Ukraine has been something of a test laboratory for hackers. The country has suffered two major attacks on its power distribution grid in subsequent years – 2015 and 2016. More recently, in 2017, the 'Petya' ransomeware attack began with infections of organizations working with the Ukrainian government, including banks, state power utilities and Kiev's airport and metro system, quickly spreading worldwide and hitting systems in many countries.[1]

The attacks show that cyber-threats are growing. It's been said there are two kinds of organization – those that have been hacked and know it and those that have been hacked but don't know it.

It's a real and present danger that has caused financial loss, but more importantly can compromise the safety of people. Mission-critical communications cannot be allowed to fail when safety is at stake.

Digital transformation is bringing substantial operational efficiency and reliability benefits to organizations running and using mission-critical communications networks. However, the adoption of interconnected IP-based systems, plus the rise in the use of internet-capable devices, increases the attack surface of mission critical networks.

Security agencies recognize the risks. In the US, cybersecurity is seen as a serious economic and national threat with the US Computer Emergency Readiness Team (US-CERT) creating a framework to support the protection of critical infrastructure. In Europe, the EU has proposed a cybersecurity strategy[2] outlining its vision, clarifying roles and responsibilities, and defining actions required to protect citizens. In Asia, some governments have established national cybersecurity policies.

Consequently, mission-critical security must be stepped up. An active security approach provides the right balance of costs with the in-depth protection needed to defend against today's security threats.

2. Lessons from past attacks

In December 2015, a major attack was launched on electricity power grids in the Ukraine, leaving 250,000 people without power. Almost exactly a year later, hackers struck again. Parts of Kiev suffered a power outage lasting about an hour. Such incidents have created some insight into how cyber-attacks develop.

In the first outage, hackers gained access to the utility's systems and manually switched out circuit breakers. But the 2016 attack is said to have been caused by sophisticated malware that could automate large-scale power outages on grids around the world[3]. The malware is built using swappable, plug-in components that could allow it to be adapted to simultaneously attack multiple targets, more quickly and more frequently than has previously been possible.

More recently, the global Wannacry ransomware attack in May 2017[4] affected more than 200,000 endpoints to cause widespread disturbance of services for organizations that included the UK's National Health Service (NHS), Telefonica in Spain, Megafon in Russia, Renault in France and Fedex in the USA.

The lesson is clear. Cyber-attacks can disrupt mission-critical services and put lives at risk.

AN AVERAGE DAY... AT AN ENTERPRISE ORGANIZATION

	4 SECONDS	**53** SECONDS	**81** SECONDS	**4** MINUTES	**32** MINUTES
EVERY	An unknown malware is downloaded	A bot communicates with its command and control center	A known malware is downloaded	A high-risk application is used	Sensitive data is sent outside the organization

Figure 1. Enterprises face constant threats from malicious software every day. http://www.internetworking.ch/files/eng-checkpoint-2015-securityreport.pdf

Anatomy of an attack … and how to prevent it

Stage 1: Break-in
The Ukrainian power system attack in 2015 began in June 2014 when hackers targeted administrative and other personnel in the power company through a campaign of phishing emails with attached documents that enabled macros to install malware.

Stopping the threat: Deploying endpoint security would detect command-and-control traffic, before malware is detonated.

Stage 2: Expand and prepare
The hackers were then able to harvest credentials and gain privileges throughout the IT system. The task was made easier because passwords were hard-coded and shared passwords were not changed regularly. The hackers set up an IPSec virtual private network (VPN) connection direct into the network.

Stopping the threat: Deploying credential protection to provide a secure point of control. Implementing anomaly protection to detect suspicious behavior. Using IP/MPLS VPN and a firewall to impede and restrict the hackers' lateral movement.

Stage 3: The attack
After about six months of undetected preparation, the hackers executed the attack, disconnecting circuit breakers and hindering recovery through a DDoS attack on the call center, blocking and wiping workstations, servers and endpoints. They also installed firmware to block remote commands. Recovery required physical visits to each substation to manually reset circuit breakers.

Stopping the threat: Deploy automated response solutions that can respond to threats before they become breaches.

3. The risks are everywhere … and many-sided

Highly sophisticated attacks like Wannacry and those in the Ukraine are likely to require the backing of a state, large terrorist group or organized crime. Such groups share the same goal: to steal information to gain a financial or strategic benefit. The motivation for groups to target mission-critical communications networks can range from a pure demonstration of force to simply gaining publicity, venting grievances, or making a political statement.

Yet these are not the only perpetrators. Up to 70 percent of security incidents are the result of some form of insider attack or error. Upset employees may use their privileged access rights to alter security configurations. Mistakes that enable IDs to be stolen through phishing attacks can lead to similar issues.

There are many different types of attack. They include data theft and tampering, eavesdropping and potentially damaging distributed denial of service (DDoS) attacks.

A fast-growing and potentially far more damaging attack is the destruction of service (DeOS) attack that can physically damage hardware and equipment by, for example, corrupting the firmware on internet-connected devices. In a power grid for instance, it is thought to be possible to overload grid components and block protective features that keep components from overheating, damaging transformers or other equipment[4].

3.1. IP and IoT increase the risks

As well as many attackers and many types of attack, there are many vulnerabilities in networks. A significant percentage of security breaches can be traced back to human error, from lack of compliance with security regulations and policies, to unintentional configuration error.

Yet, the evolution of communications networks to IP technologies, the increasing use of IP-based applications and the growing adoption of Internet of Things (IoT) technologies are widening the spectrum of vulnerability.

In the past, systems tended to be isolated, providing natural breaks that could stop the spread of a malicious infection or the reach of an attack. However, today's IP-based applications and the underlying mission-critical networks are more interconnected, increasing their vulnerability.

Furthermore, the need to run IP networks alongside legacy network technologies, such as SCADA, adds further security complexity. A good example of how legacy vulnerabilities can carry forward into today's systems is Signaling System No. 7, or SS7, which was designed more than 40 years ago. The underlying methodologies for the SS7 signaling protocol, as used in TETRA for example, have been incorporated into Diameter, a protocol used in standard IT-based, packet-switched/Ethernet-based solutions, including LTE wireless networks. As a result, security threats to SS7 networks may also be possible in LTE networks, requiring increased security on signaling interconnects.

Meanwhile, the growing use of sensors, meters, surveillance cameras and other devices to support real-time monitoring and situational awareness, improves operational efficiency, reliability, resiliency and safety of critical infrastructure. On the flip side, a growing threat this evolution brings about is the risk of cyber-attackers gaining control of IoT devices and using them to run malware to launch different attacks, ranging from spam to data theft to DDoS.

Indeed, it is possible, even likely, that there are many installed devices today that have been compromised, yet their infection is undetected because they continue to perform their intended functions. A hacked sensor could be sending millions of spam messages per month over a long period of time, but this may not be obvious unless the IP address range is blacklisted.

In October 2016, attackers managed to hack 145,000 IoT devices to execute the largest distributed denial of service (DDoS) attack to date[5]. The attack, using a weapon called the Mirai botnet, affected a wide range of organizations from Paypal to Twitter, to Amazon to Spotify. While it did not directly target mission-critical networks it does show how smart sensors are a prime target for manipulation.

3.2. IP-based wireless networks need extra protection

A further development is the adoption by mission-critical organizations of wireless networks in the shape of LTE and future 5G technologies. LTE security is based on two layers of protection instead of one-layer perimeter security as in 3G. The first layer deals with security in the radio access network, while the second layer provides security in the Evolved Packet Core (EPC) network. In practice, the implementation of this two-layer security architecture is subject to vendors' interpretation and therefore, may expose a mission-critical network to threats if not engineered properly.

The encryption of all traffic between base station and core network is also essential. LTE networks provide hop-by-hop protection that could lead to the possibility of security being compromised by incorrect system configuration parameters. End-to-end encryption provides protection for situations where security is not configured properly in LTE equipment.

In public safety and other mission-critical networks, voice services depend on group communications in which users can simultaneously communicate, walkie-talkie style, with groups of other users. These require specific security arrangements to enable secured group call communication, direct mode of operation, security of both device and back end control servers.

4. Defense in depth is vital to protect mission-critical operations

Cost-effectively protecting mission-critical networks from cyber-attack first requires an understanding of the risks to the specific networks and their underlying operational processes to define the scope and appropriate level of protection required. Even if a completely airtight, secure network would be possible, it would require an unrealistic level of investment. Rather, defense in depth is a more balanced, economically feasible approach to provide the necessary security to mitigate the real risks.

The aim is to build cyber defenses aligned with the network's operational objectives. They must focus on processes and technologies to implement effective layered security across network, application, data, identity and access management, laying a series of defenses to thwart attacker's attempts to exploit security gaps.

Humans also play a predominant role in cyber defense. Supplementing all security measures in place, mission-critical operators need to train all employees to be prudent in electronic communications and be vigilant about reporting any anomalies, reducing security risks and protecting the mission-critical systems.

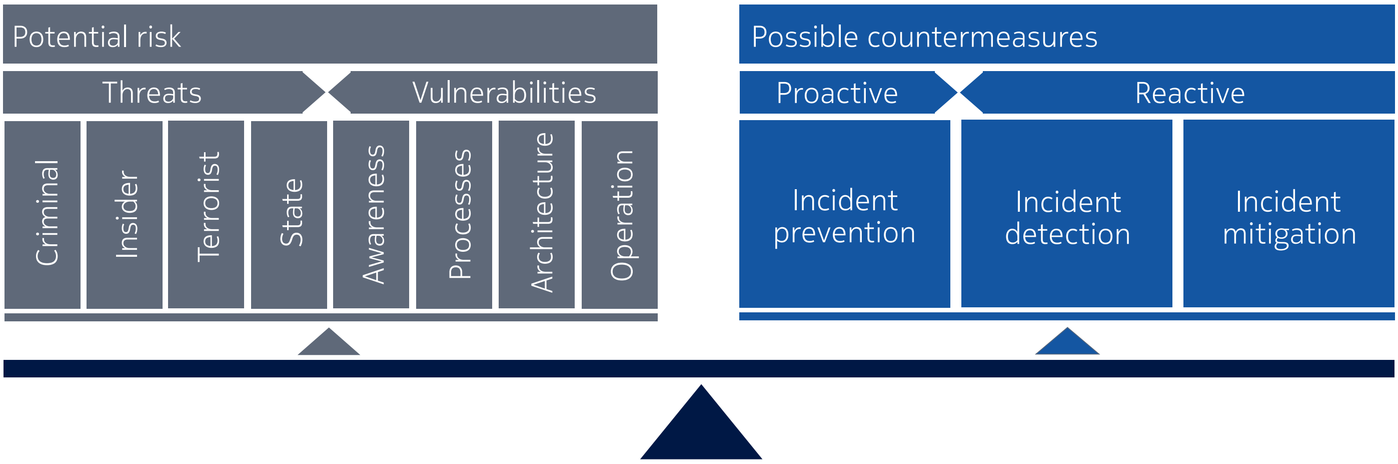

Figure 2. Security always requires a balance between the risk from threats/vulnerabilities and required investments for countermeasures.

5. Essential elements of in-depth security

There are some basic elements of effective cybersecurity for mission-critical networks.

Automate security processes: First, today's manually-intensive incident response approaches need to be automated. It's not uncommon for large critical network service providers to be bombarded with thousands of cybersecurity alerts every day. Not all will be security breaches. Many will be false alerts and duplicate information. Yet, the sheer number of alerts can overwhelm a security team, leading to serious incidents not being followed up. They need better ways to automatically correlate, prioritize and deal with these alerts.

Furthermore, current approaches are inefficient, with up to 33 percent of incident response time spent on manual processes, leading to delays. Combined with alert fatigue and time wasted on false calls, many security breaches can go undetected. Security automation that encompasses business processes, regulations and security policies will be essential to keep pace with the rapid rise in attacks.

End-to-end security is essential: End-to-end security is vital to protect both the IP and LTE components of communications networks. Failing to address this will result in inadequate network protection and increase vulnerabilities to threats that are specific to one technology or the other.

End-to-end security encompasses the operation of the entire network and its security processes, such as access management and audit compliance; network security, including signaling and core network security. In addition, security management for IoT devices must include three key components: secure identity management for each device, a secure communication channel between the management server and the devices, and a secure trusted software environment on each device.

Network segmentation and firewall: Network segmentation with IP/MPLS VPN by applications or other policies provides traffic isolation and hampers lateral movement of hackers as they scout the infrastructure. The firewall also restricts illegitimate traffic from flowing in the networks.*

Analytics for continuous improvement: Security analytics correlates data from across the network, devices and cloud layers to spot suspicious anomalies and provide insight into the nature of the threat, the associated business risk and recommended response. With machine learning, the effectiveness of security would increase continuously.

Encryption protects data: With encryption, even when a perpetrator taps into the communication channels, confidentiality, integrity and authenticity are still protected. As the network is deployed with different architecture and transport technology, it is vital to deploy a flexible multi-layer encryption that safeguards traffic at the IP, MPLS and transport layer as necessary. Encryption should also be applied to stored data, not just when it is being moved around.

High availability: Ensuring high availability and operational stability of the network and transport layers (for example on IP/MPLS, DWDM) is a key foundation for a secure network because it enables a rapid recovery from attack, including physical shut down of communications equipment and infrastructure facilities.

*For more detailed information see: Impregnable network defense for mission-critical networks
https://resources.ext.nokia.com/asset/194791

5.1. Implementing active security management

Various standards relating to security are available (see text panel "Standards for security"). There is also a wealth of best practices from mission-critical networks around the world, most of which advocate an active security management approach with automation and continuous improvement.

The traditional approach to security is largely based on manual processes without a centralized management system. This is still a reasonable approach for some organizations, but the increasing sophistication of attacks and growing regulatory complexity mean this will not be realistic in the medium term.

An expanded security management solution with analytics, automation and reporting would support workflow management and automation, analytics and reporting. This would enable security operations teams to automate and prioritize activities and report data to inform better business decision making.

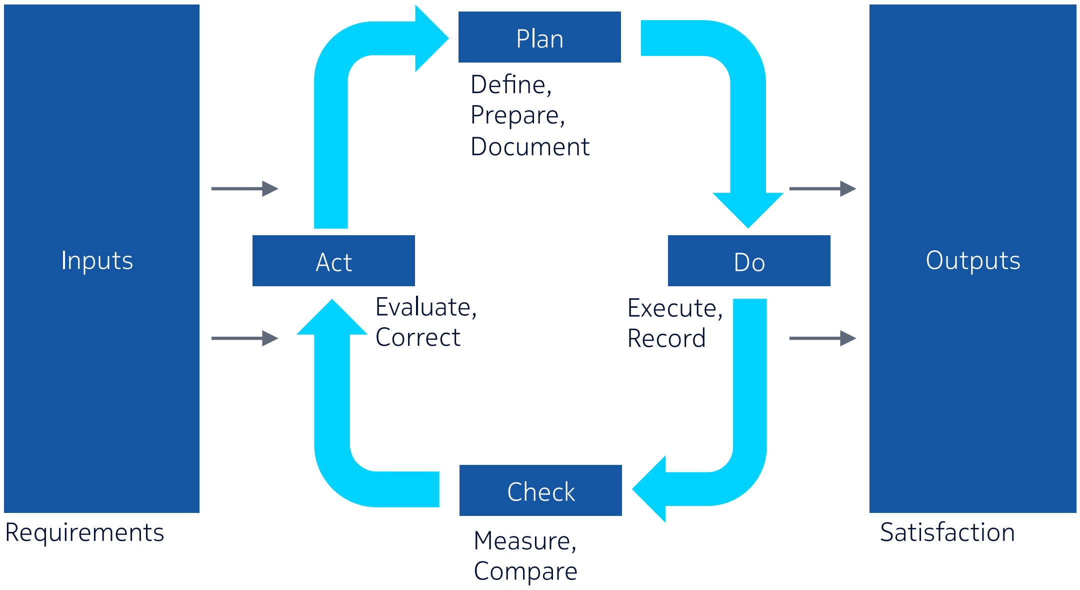

Figure 3. ISO27001 is typical of the active security management approach to cybersecurity.

Standards for security

Examples of relevant security standards include:

ISO 2700x Information security management systems – ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

ITU-T X.805 security architecture - a streamlined high-level threat model, enabling operators to assess network security and eliminate potential threats in complex environments. It can be applied across network operations, as well as in network management.

There are three layers to the architecture:

- The infrastructure layer, which comprises basic communications network building blocks such as routers, switches and transport equipment.
- The services layer, which comprises network services or circuits that deliver data generated by applications, such as Supervisory Control And Data Acquisition (SCADA), Land Mobile Radio (LMR) or closed-circuit television (CCTV), end to end across the communications network.
- The application layer, which comprises the devices, or simply known as endpoints, over which applications such as SCADA, video surveillance and IP telephony run. The endpoints could be a SCADA RTU, CCTV camera, SCADA server and Video Management System (VMS). An endpoint includes all associated hardware, software and firmware.

IEC 62443(-2-4) Security for industrial automation and control systems (IACS) – specifies requirements for digital security capabilities for IACS service providers during integration and maintenance of an automation solution.

6. Nokia cybersecurity for mission-critical networks

Nokia offers in-depth expertise in the development of cybersecurity best practices. Mission-critical networks solutions not only deliver network reliability, performance and scalability, they also defend against security threats and attacks.

The approach to mission-critical cybersecurity recommended by Nokia is based on a security framework that aligns an organization’s different working groups and implements common best practices. The ITU-T X.805 security framework is used to help operators improve end-to-end network security and eliminate potential threats in complex, dynamic environments, and it can be applied across network operations and management.

Nokia end-to-end security solutions incorporate security products and services that address the specific challenges of mission-critical network operators. For example, the Nokia Netguard Security Management Center and Security Operations Analytics and Reporting platform enables security operations teams to automate and prioritize activities and report data to inform better business decision making.

Critical LTE communication networks need to participate their own defense. This self-defense capability is best developed during the product design phase. The Design For Security (DFSec) approach used by Nokia deals with proactive security measures, including risk and threat analysis, secure OS configuration, access control, password policy, code review, penetration testing and other activities. Nokia also implements reactive security measures known as security vulnerability monitoring (SVM) to ensure that OEM product vulnerabilities listed by computer emergency response teams (CERTs) are highlighted for further qualification and possible patches.

Nokia combines expertise in both LTE and IP to achieve mission-critical security that addresses the vulnerabilities specific to LTE technology. Nokia integrates security seamlessly with the existing operations support system (OSS), providing the relevant alarms, counters and monitoring capabilities without additional terminal applications or equipment. This enables the operator to focus on its mission-critical responsibilities without being distracted by the daily running of a telecom business or by having to work with multiple security vendors to align on security roadmaps or incident resolution.

Nokia services provide the expert support operators need to secure their communications networks. For example, the Nokia Security Risk Index (SRI) assessment framework and Managed Security Service (MSS) encompass all areas of security, including the assessment and continuous protection of multi-vendor networks.

Nokia works with operators around the world to develop proactive cybersecurity protection for mission-critical networks. Nokia security expertise is rooted in its strong presence in the public safety segment and as a trusted partner for public network operators around the world which impose the highest requirements for network security.

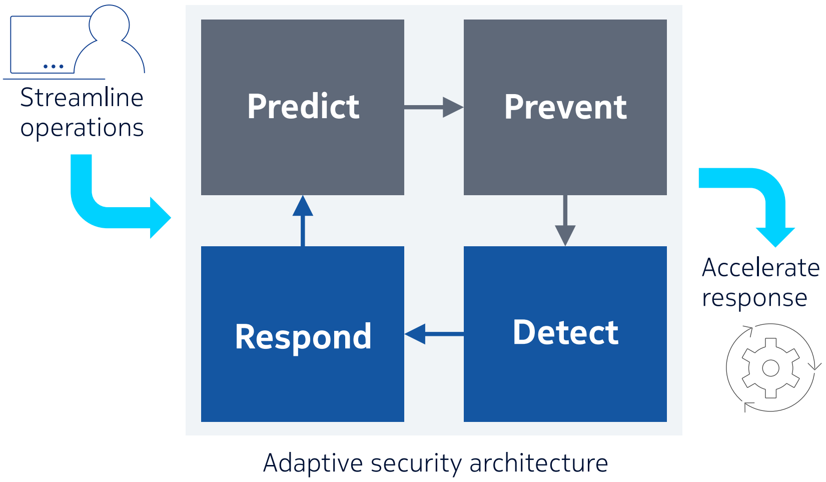

Figure 4. Security orchestration analytics and response transforms railway communications network security from manual and reactive to dynamic, predictive and automated.

Keeping Dubai's smart city secure

Nedaa, Professional Communication Corporation, the Dubai Government security networks provider, and its approved technology provider Esharah Etisalat Security Solutions, have commissioned Nokia to deploy a smart city solution based on a 5G-ready next-generation network.

This latest project with the Government of Dubai builds on Nokia's existing working relationship with the city. In 2001, Nokia started to work with public safety communication networks in Dubai, and the current project will be a continuation to keep Dubai a safe and smart city for its residents and visitors.

Yousif Al Ali, Nedaa CTO, said: “Nokia has been an integral part of Dubai's security communications network since 2001, and the company's eagerness to adapt to our new, stringent security requirements gives us the confidence to make our city the safest and smartest in the world.”

7. Conclusion

Hardly a day goes by without the media reporting a cybersecurity incident or exposure of a risk somewhere in the world. Not only are attacks becoming ever-more sophisticated, but the potential damage that can result is growing, even physical damage to critical infrastructure such as electricity distribution grids.

Mission-critical networks can ill afford any successful cyber-attacks. Not just financial loss is at stake; lives can be put in jeopardy.

At the same time, it is important for mission-critical communications operators to evolve their networks towards new networking technologies, including LTE, IP/MPLS, packet optical and packet microwave, to support new services and improve the efficiency of their operations. While such networks are future-proof and scalable, they will introduce new vulnerabilities. With a robust network defense, these threats can be addressed.

Deploying the right level of security is a high priority. While all mission-critical networks are different, sound security typically requires a move from manual processes to automation, the application of data analytics and machine learning, as well as end-to-end encryption.

Nokia offers an advanced and comprehensive approach that is built on its long experience and in-depth expertise of both security and mission-critical networks and operations. In line with best practices and published standards, the Nokia solution can ensure the highest levels of protection for mission-critical communications.

Enterprises and the public deserve nothing less.

8. Abbreviations

CCTV	Closed-Circuit Television
CERTS	Computer Emergency Response Teams
DDoS	Distributed Denial of Service
DeOS	Destruction of Service
DFSec	Design for Security
DWDM	Dense Wavelength Division Multiplexing
EPC	Evolved Packet Core
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Internet Protocol
IP/MPLS	IP Multiprotocol Label Switching
ISMS	Information Security Management System
LMR	Land Mobile Radio
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
OSS	Operations Support System
SCADA	Supervisory Control and Data Acquisition
SS7	Signaling System No. 7
VMS	Video Management System
VPN	Virtual Private Network

9. References

1. https://www.us-cert.gov/ncas/alerts/TA17-181A
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
3. https://www.wired.com/story/crash-override-malware/
4. https://www.us-cert.gov/ncas/alerts/TA17-132A
5. https://www.siliconrepublic.com/machines/internet-meltdown-mirai-botnet

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code SR1802021640EN