IMPROVING CYBERSECURITY

– How to defend against cyber threats and safeguard operations

An overview of the key findings, recognised challenges and proposed solutions based on VTT-led research project, KYBER-TEO

VTT Technical Research Centre of Finland Ltd, 2017

KYBER-TEO is a set of projects led by VTT, in which the National Emergency Supply Agency and several industrial pioneers and cybersecurity service providers came together in 2014–2016. The project was supported by the National Cyber Security Centre and Tampere University of Technology. Participants joined forces to identify key challenges and develop tested methods and best practices.

This summary will enable industrial operators, system and software companies and service providers to acquire cyber-secure automation systems and develop their own cybersecurity guidelines and policies to ensure continuous operations.

Contents

The increase in cyber threats and advanced attacks

The need to prepare for cyber threats is increasing as businesses and industry become more dependent on automation systems. Integrated systems, functions and collaboration networks are becoming more complex.

New types of cyber threats:

- spreading of and making money from ransomware
- disinformation based on fake media and news
- illegitimate remote access and exploitation of IoT devices
- abusing dual-use products (using test tools to mount attacks and strong encryption to evade the authorities)
- increase of state-controlled online intelligence activities

Today, online criminals have access to highly sophisticated technologies and their own closed communities, in which they are developing new communal ways of generating illegal profits via information networks. A vast amount of criminal service business has evolved in the sector and criminals have even put malware and attack software into "production use."

Industrial operators, system and software vendors and authorities must continuously learn about new cyber-world tools and actively develop increasingly efficient methods of identifying and preventing online crime. The cybersecurity requirements of information systems and networks are continuously evolving, and updates and enhancements must be deployed one after the other. For this reason, it is crucial that businesses ensure their own cybersecurity expertise is at a sufficiently high level.

A holistic approach is required in order to react effectively to the challenges posed by online and information system security. In addition, sharing experiences learned the hard way is a prerequisite for future continuity.

Increasing regulation demands more development work

Cybersecurity threats are being prepared for at European Union level, through measures such as legislative changes and supplementing the requirements of EU directives. The directive on the security of network and information systems, the so-called NIS Directive, sets new requirements for ensuring high-quality online and information system security.

The NIS Directive applies to critical infrastructure in particular and imposes specific obligations on the following industries:

- energy
- transport
- banking
- financial market infrastructures
- healthcare
- water supply and distribution
- digital infrastructure

With the introduction of the NIS Directive, key service and digital service providers will have common security requirements. Operators and suppliers in the field of security of supply, in particular, can expect concrete requirements and sanctions that will revolutionise security-related policies and the amount of development work needed.

The directive is expected to result in the definition of “minimum-level” security controls, and will promote the confidential exchange of information in cybersecurity events throughout the European Union.

CHALLENGE 1: Insufficient management of production assets

Production assets and intellectual property are targets of serious cybersecurity threats. Identifying and monitoring changes and vulnerabilities that pose a threat to the normal state of the system needs to be done preferably in real time. Reliable and efficient monitoring requires automatic methods and tools.

Management of production assets plays a key role in cybersecurity, because cyber threats are increasingly being targeted at critical production and intellectual property and correct system operation and configuration. Production asset management and monitoring enable an up-to-date view of the situation regarding cyber-vulnerable targets.

Need for electronic monitoring

To ensure a response to cyber threats, it is vital to have a continuous view of a situation. This generates the need for continuous physical and electronic monitoring.

- Are production tools still in the right places and running?
- Does the configuration of production tools correspond to a secure state of affairs?
- Are there activities, devices or software in the production network that do not belong there, and that may involve intelligence or corporate espionage?

These all are questions to which answers are sought through automatic vulnerability and threat management methods and tools.

Monitoring of production assets

Credible monitoring of production assets requires continuous work and strong competencies. Automatic monitoring tends to be quite problematic or labour-intensive to set up and maintain. Monitoring technologies are still being developed and may themselves increase the threat, if monitoring cannot be managed safely and its correct use controlled. Commissioning is slowed down by insufficient competencies in new technologies.

Lifecycle thinking as a requirement

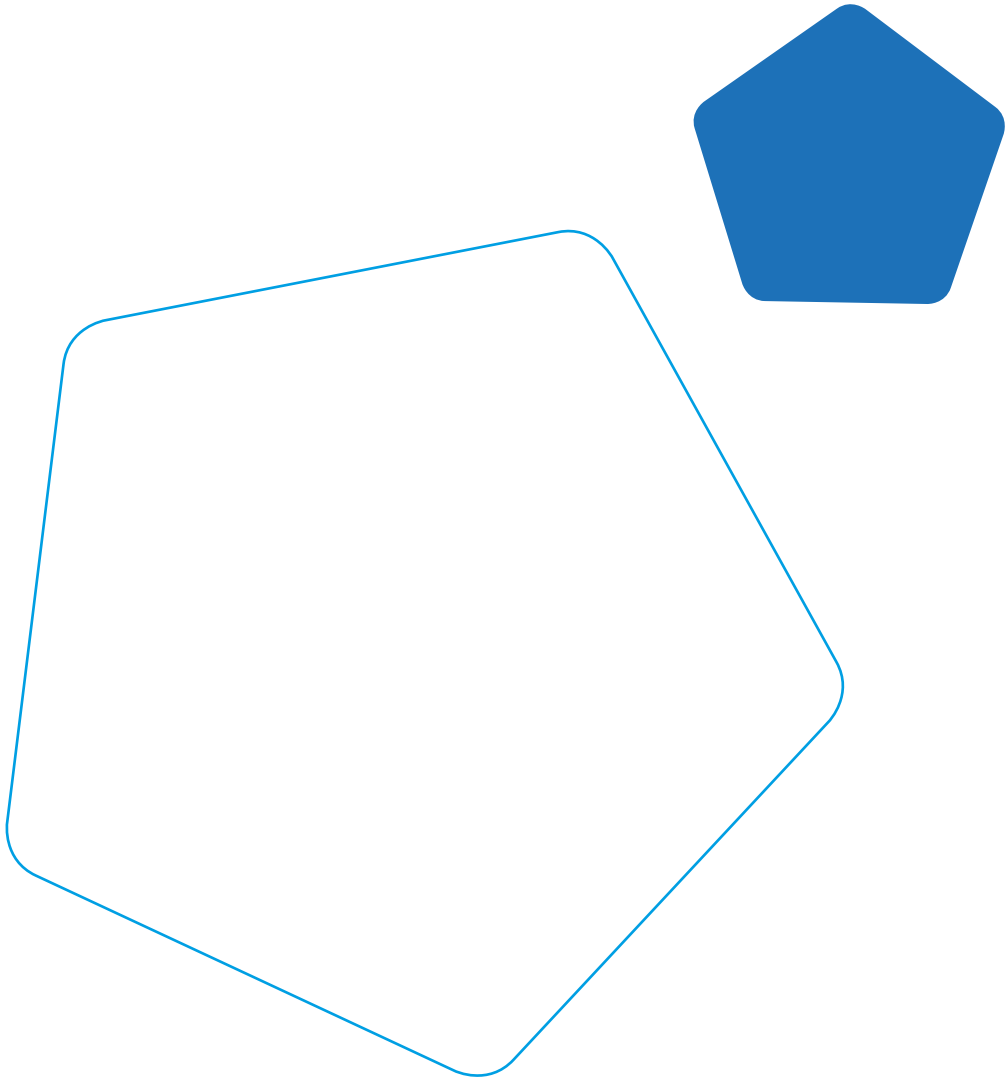
Cybersecurity must be included as part of the entire lifecycle management of automation, in order to develop and maintain cybersecurity and continuity. Management of production assets must support the cybersecurity situational awareness throughout the lifecycle:

- preparation of cybersecurity plans (what is to be secured?)
- management of vulnerabilities (what products are in use?)
- management of cyber threats and anomalies (manage the targeted objects)
- monitoring and distributing cyber-safe configurations (distribution management)

Identifying threats

The systematic identification of vulnerabilities in and threats to production IT systems requires the appropriate ownership; participation in forums; management of vulnerabilities, threats and anomalies; and tools:

- Mapping, documenting, monitoring and in-depth understanding of the correct operation of production IT systems.
- Data collection and sharing in applicable forums for monitoring vulnerabilities and threats.
- Monitoring and identifying cybersecurity vulnerabilities and determining their applicability to production.
- Monitoring and identifying cybersecurity threats and determining their impact.
- Tools with which networked systems can be systematically and automatically monitored and problems identified.



CHALLENGE 2: Increasingly complex architectures and technologies

With growing threats, the production environment needs to be well secured. It is necessary to strengthen telecommunications, security zones between data and computing, and safe implementation and monitoring of subnets and virtual environments.

A monitored automation network architecture is needed at the latest when the industrial Internet, free bands and wireless data transfer in mobile networks enter production.

Ensuring cybersecurity requires the secure implementation and maintenance of gateway devices and software and wireless networks (e.g., building automation applications) and behavioural monitoring.

Architecture analysis

The cybersecurity of various architectures and concepts included in the implementation of an automation system must be separately analysed.

Ecosystem architecture choices for an automation solution are often determined based on the business goals of key ecosystem operators, and partly through networked development as well.

The possibilities and threats related to various options should be determined and assessed. Could, for example, dependence on a specific ecosystem pose unreasonable threats to one's own business later? In the current security and economic environment, which is prone to major changes, it may be difficult to assess this.

In production development projects it should be determined who analyses alternative architectures and when and how they will be fixed between the client and suppliers. Issues to analyse should include the:

- physical and logical data network architecture
- telecommunication architecture
- automation system architecture
- intelligent device implementation architecture
- automation software and application architecture
- management or maintenance architecture
- information security architecture
- monitoring architecture etc.

Problems with commitment

If corporate espionage and infiltration commissioned by state operators are considered a real threat, companies working on security of supply must take into consideration these risks in their own ecosystem choices.

How will trust in security and competitiveness develop for companies whose head office or automation systems are located in the United States, Sweden, Japan, Germany or China, for example?

As a precaution, backup systems should be independent of the main system vendor, with respect to both technology and geography, as well as politically. For example, telecommunication arrangements typically require separate backup systems with terminal devices, networks and carriers.

Assessing remote access concepts

In production, the secure remote access concept must be defined at company level, as it is one of the key principles or rules that also affect other architecture choices.

In particular and in principle, the production remote access concept must, for example, deny continuous, end-to-end encrypted VPN connections from the vendor's network to the plant's automation device. Such a policy could have a significant impact on standard procedures and solutions in automation and equipment suppliers' remote maintenance services, and should be discussed with vendors well in advance.

CHALLENGE 3: Unclear division of labour and procedures

The high number of operators and tasks during the production lifecycle generates cybersecurity risks, the identification and management of which require continuous work. All operators must be included in the development of cybersecurity and various steps must be taken to ensure that they have sufficient cybersecurity expertise.

This is often learned the hard way. For example, a subcontractor's employee working on the maintenance of a production system may casually bring a computer containing malware into the production area, causing malware to spread throughout the customer's production network. An intelligence process that has progressed in this way may not be identified because unauthorised prying in the internal network is not even suspected, so the "contamination" is not detected immediately.

The division of roles needs clarification

CPNI, the government authority for providing protective security advice to the UK national infrastructure, defines a place in the production lifecycle for every party essential to cybersecurity.

This idea is worthy of consideration; the division of roles between different operators is in particular need of clarification. Sufficient cybersecurity competencies among all parties, the clear division of responsibilities and the availability of outsource services, updates and fixes must be ensured as early as the ordering stage.

It regrettably often transpires that the development and sharing of internal employees' competencies are insufficient. In many cases, only one person knowledgeable in cybersecurity is hired, with all of the related responsibilities being assigned to that person. This is rarely a long-term solution.

Actual cyber threats prove that cybersecurity must be considered at all stages of the automation lifecycle: from the preliminary study and specification to the decommissioning of a system, device and software that have served well.

Considering cybersecurity in automation procurements

Cybersecurity must be included in all automation procurements. Development investments have the greatest impact during the procurement phase of automation. Key cybersecurity requirements must be presented to automation and machine vendors, and only services and products that are cyber-safe must be chosen.

The most functional and, thus, most cost-efficient method of managing cybersecurity is attained by developing and testing working methods in good time. In this scenario, no unexpected cybersecurity threats can enter production systems by automation systems and the related maintenance measures. Active ownership and continuous risk management are required in order to ensure continuity.

	Product development	Procurement	Testing and commissioning	Production and maintenance	Decommis-sioning
Orderer	Ensures the continuity of the partnership network	Leads, sets responsibilities and requirements	Plans and monitors implementation	Manages and monitors compe-tence, property, risks and changes	Defines the decommis-sioning permit and process
Primary project vendor	Manages the security require-ments of the project	Divides the tasks of the delivery agreement	Co-ordinates and monitors the project testing	(Maintains documentation)	Implements
Integrator	Manages the security require-ments of the integration	Documents the security of the integration	Ensures the security of the integration	(Maintains documentation)	Implements
Automation system vendor	Ensures and tests the security of the technology	Describes the security of the system	Hardens, tests and trains the delivery	Maintains, repairs, reports, investi-gates and recovers the hardening	Implements
Hardware, application, software vendor	Ensures and tests the security of the technology	Describes the security of the system	Hardens, tests and trains the product	Hardens and tests the product	Implements

Responsibility assignment matrix

Preparedness plans in production

To secure services during the entire lifecycle, the production function must make its own preparedness plans and build a reliable network of partners.

Because cyber threats evolve quickly, continuous risk analysis is necessary and plans must also be maintained in the production and maintenance phases. Each operator must be familiar with secure methods in its own work and act accordingly.

The main cybersecurity tasks must be defined for each operator throughout the automation lifecycle. All operators, from production engineers to janitors, must be included in the security-maintenance circle. They must understand the grave consequences of negligence and adhere to cybersecurity instructions and safe policies. Negligence by a single operator can destroy all of the work done to improve security.

Solutions for promoting cybersecurity

Developing cybersecurity solutions that ensure continuity of production requires effective collaboration and improved awareness of the cyber threat and division of work among key vendors throughout the lifecycle.

If the cybersecurity of automation is developed solely from the ICT perspective, a dead end will result during the commissioning phase at the latest, when it is noticed that the solution is not applicable to established practices or conditions in the industry.

The best solutions are based on broad-scale collaboration between sectors and companies, and the utilisation of broad competencies. The solutions and best practices listed below have been developed and verified in collaboration with pioneering companies in the sector.

Improving awareness in businesses

Cybersecurity continues to grow in importance to society as a whole. First, threats must be recognised so that sufficient effort can be made to thwart them.

We have grown highly dependent on the availability of public information networks and faultless operation of online services. This has been proven by several denial of service attacks caused by cheap consumer devices connected to the Internet, ransomware targeting the healthcare sector and other threats.

Various threats are becoming ever more commonplace:

- cybercrime
- cybervandalism
- hybrid threats (critical infrastructure)
- terrorism and terrorism planning

Companies are also subject to threats through employees and people close to them. This is due to phenomena such as the use of mobile devices for both work and leisure and the widespread use of the social media applications. For example, opening a link recommended by a friend or relative may lead to the undetected installation of a malware application on a work computer.

Promoting cybersecurity awareness

Awareness building aims to facilitate the deployment of cybersecurity within companies that develop and utilise automation. The culture of silence around computer break-ins has significantly hampered risk awareness among executives.

Development does not begin by itself. It requires:

- an active leader
- thorough familiarisation with the general field of cybersecurity
- identifying the company's own, special problems and
- commitment at executive level

The company's head of development or information security, if such a person has been appointed, may be an inhibitor or catalyst. The first requirement is sufficient dissemination of awareness so that all employees understand the nature and propability of cyber threats.

Only after this can a company begin the specification of responsibilities and resource allocation, in order to identify and prevent cyber threats to production and to prepare for them in advance.

Company-internal cybersecurity seminar

A cybersecurity seminar is an effective way to improve company-level awareness. The seminar can be used to illustrate the ways in which automation systems have previously been breached, what types of tools, services and social engineering the attackers are using and what kind of damages have been caused.

PART 1: BASICS

Comparing the cybersecurity of automation and IT information security

Present state of automation cybersecurity

- In what ways have automation systems previously been broken into?
- What types of tools, services and social engineering do the attackers use?
- What kind of damage has been caused in this way?

Cybersecurity status of automation

- What are the current trends with respect to developing information security in automation?

Duties, roles and division of labour in cybersecurity within the automation lifecycle

- Overview of the division of labour in cybersecurity
- Key tasks: orderer (procurement, IT, automation etc.), project vendor, system vendor etc.
- Discussion of the company's own division of work

PART 2: DEPLOYMENT EXAMPLES AND DISCUSSION

Examples of deploying information security in production, for example:

- Cybersecurity requirements and procurement instructions
- System hardening during the automation lifecycle
- Cybersecurity testing and development of automation
- Examples of the deployment of cybersecurity measures in other companies

Questions, discussion, further measures

An example of the content of a cybersecurity seminar that greatly promotes awareness.

Emphasising the cybersecurity situation of automation in particular, as well as acute cybersecurity threats and trends, can stimulate internal discussion among staff and management. Ideally, this could lead to the establishment of cybersecurity development groups.

Instructions, requirements and division of roles

A clear security policy and simple instructions are the foundation for developing and maintaining cybersecurity, particularly in multiple vendor environments.

Enforcement of the overall security of operations and adherence to instructions must be carefully monitored and developed.

A good cybersecurity policy takes account of a company's business model and the results of risk analyses; combines cybersecurity with other security and continuity elements; is easy to understand, logical and well-communicated; and serves as a foundation for the preparation of more detailed cybersecurity instructions.

Detailed cybersecurity policy

Cybersecurity cannot be copied from others. Instructions appropriate to the threats and production practices of a company must be separately tailored for each personnel segment and investments must be made in communication and implementation. Cyber-security policies serve as rules with which an organisation can secure its sensitive and critical system resources. Adherence to the rules can be audited with reference to the rules and process descriptions.

The applicable sections of the IEC 62443 standard and the cybersecurity policy templates of the SANS Institute (www.sans.org/) can also be used when preparing the policy. The IEC standard and the SANS templates are mutually complementary; combined, they offer a valuable basis for creating and updating a company's production cybersecurity policy.

Working instructions

It is often also necessary to prepare concrete instructions on handling cybersecurity incidents. Such instructions must cover issues such as the actions to be taken when something out-of-the-ordinary is observed, including urgent measures, reporting, investigation, recovery to normal state and learning from the incident.

Updating of instructions

With respect to the commissioning of new technologies, a separate analysis is needed to determine whether changes or updates are needed in the cybersecurity policy. For example, companies using the industrial Internet may face the risk that IoT devices are unobtrusively installed in the internal network and the cyber threats they pose are not noticed until later.

Versatile local area network management tools are often introduced because of their monitoring and diagnostics features. To prevent abuse, the use of such tools must be restricted to specific maintenance purposes, tasks, devices and access rights.

Cybersecurity testing

The testing of automation systems to prevent information security vulnerabilities is gradually gaining interest among global industrial operators. End customers, too, are asking automation system manufacturers to provide cybersecurity test reports, certificates and proof of appropriate implementation.

Fairly few systems have proven to be cyber-safe, and they are too expensive for many. Most automation system vendors and machine manufacturers perform at least one-off information security testing on their products. This, however, is not enough.

Finland has skilled automation developers and reliable and developing cybersecurity service and product providers. It has been necessary to combine these to secure the development of cybersecurity testing.

Prerequisites for testing

The main goal of cybersecurity testing is to make automation systems and their support systems sufficiently safe during the development phase. No faults or vulnerabilities, which might be exploited later, must be left in products.

This requires cooperation between system vendors and testers and the determination and development of matters such as the following:

1. FUNCTIONALITY: the most detailed possible knowledge of the correct functionality of the test object, including automation functions
2. COVERAGE OF TESTING: determining realistic test coverage and dividing testing into different types of periods, so that the most critical functions can be tested
3. QUALITY OF TESTING: determining the most efficient test tools and methods applicable to the test object and competence development
4. DEPTH OF TESTING: using applicable test methods and tools to drill down into the particular problems of the test object
5. IMPACT OF DIFFERENT PLATFORMS AND INTEGRATIONS: understanding the various uses and installation environments of the test object This may provide indications of hidden, critical interfaces and functionality.

When running, an automation system must not reveal too much system information, in order to make it as difficult to attack as possible. The attacker must be taken into account during system design, when determining whether system data and fault codes should be included in the responses to system queries, or how the system will respond to various port queries. It must be as difficult as possible for the attacker to determine what ports are used for each automation function.

Reliability of the tester

It is very important, although difficult, to ensure the reliability of the tester. The orderer must assess whom they will trust and who will test their system and design information, if any.

Trust will grow gradually through increased co-operation. In practice, this may take

several years and include different forms of co-operation and, for example, joint projects in which the number of shared tasks can be increased as trust grows.

Trust in a certain company will, naturally, vary by country, as each country may have its own intelligence services and different laws on intelligence and privacy. Reliability must come first, and “operational integrity” must be continuously evaluated.

The reliability of the tester can be assessed using methods such as the following:

- requiring basic-form security clearance
- requiring a strong and long-term non-disclosure agreement
- requiring training on ethical hacking or similar
- using the original sources to verify the references presented by the tester
- assessing security on the basis of previous co-operation

Applicable test methods

Various test methods are applicable to testing the cybersecurity of automation. They should be applied together with the deployment instructions.

Source code analysis: identify weak points in source codes, such as vulnerable commands, with the aim of reducing their numbers during the programming phase.

Secure software design processes and programming rules (for example, SEI CERT coding standards) create the foundation for producing faultless software. The entire R&D environment must be protected both technically and using procedural instructions. For example, a workstation must never be used for hobbies, as this creates exposure to a range of threats. Automation programmers must be trained to use safe software libraries and protect themselves against unauthorised prying, for example. The source code of automation applications should be automatically analysed during the compilation phase. A suitable source code analyser should be installed in the development environment.

Fuzz testing: send non-standard inputs to the target interface.

In most cases, this method is very efficient at detecting automation programming errors and is also suitable for identifying zero-day vulnerabilities and testing denial-of-service attacks.

The network traffic of a communication interface corresponding to the test object is recorded and modelled so as to identify the allowed inputs. During testing, inputs are varied and entered into the test object’s interface, while observing the object’s behaviour and responses. Many tools will automatically record non-standard behaviour in the test report. The most efficient way of achieving this is to use a protocol tester, which has been developed specifically for the automation protocol supported by the test object.

Port scanning and network sniffing: the information network and devices connected to it and their open communication ports are systematically searched.

Finding open communication ports is a highly suitable method of testing hardening. If a port does not respond within a specific time, the tester usually assumes that it is not being used. However, scanning test tools may not find all ports in use based on the standard settings, as communication ports may be used in a different way than in normal Ethernet traffic. It is difficult to identify the correct settings of a tool without thorough knowledge of the automation system being targeted.

In network sniffing, traffic in the network is passively listened to, or queries are actively sent in order to identify the devices in the network. This is a way of identifying services belonging to the automation network and those that do not belong there.

Vulnerability scanning: software vulnerabilities are searched for in the network and in devices connected to it.

Vulnerability scanners automatically inspect the software versions of systems in the network, by sending simple messages to the communication interfaces of the target systems. Vulnerable systems are found when the tool compares responses from the network with known vulnerable versions. In many cases, non-updated software versions are still used in automation and vulnerabilities can be identified without scanning.

Care must be taken with the use and settings of these tools, as certain vulnerability scanners may automatically exploit vulnerabilities.

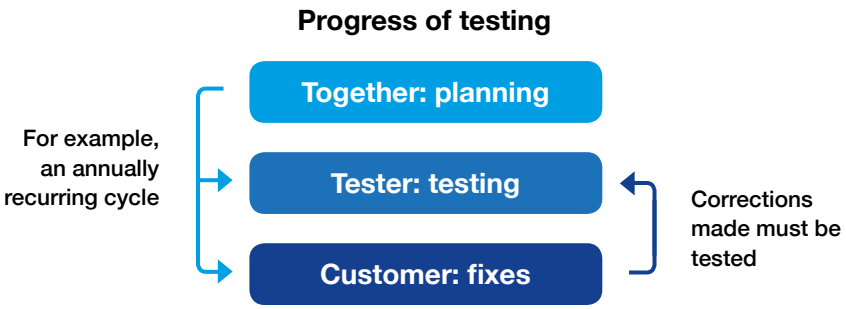
Penetration testing: attempt to break into the target system using all of the methods and tools. All means of breaking the target can be used.

Several attack tools are available. Social engineering means are also often included in penetration testing, whereby even human behaviour can be tested in order to assess the attack resistance of the target. Services related to automated production can also be tested.

It is recommended that the automation system be tested in a closed test environment. This enables the safe and versatile use of test methods and the development of test automation.

Progress of technical testing

External help is often needed in the cybersecurity testing of automation systems.



A simplified chart of the progress of confidential testing in technical proofing.

Begin by jointly designing the targets and use cases to be tested and, in particular, the content of the testing: what methods and tools will be used for the testing and how extensive will the testing be.

After this, the cybersecurity tester will perform the testing and write a test report. The best result is often obtained based on several testers and the opportunity to consult the customer, regarding the correct behaviour of the test target during testing for example.

After this, the customer will repair or have a third party repair its products according to the findings. A product that has been patched should be re-tested to ensure that the faults have been eliminated and the patches did not contain new vulnerabilities.

Fixing vulnerabilities

The goal is often that the customer itself can test and fix the majority of typical vulnerabilities. This requires moving onto the next phase, where cybersecurity testing is automated and deployed as part of the developer company's product development process.

This, however, is demanding, as cybersecurity testing methods and tools are continuously evolving, which will most probably necessitate continuous updates and testing of the integrated test tools as well.

Production monitoring

The data networks of the production unit must be monitored to ensure undisturbed production, prevent network faults and ensure asset management and sufficient capacity.

To create a comprehensive view of the state of cybersecurity in the network, you should determine whether production works exactly as planned, or whether changes have occurred. Problems concerning the normal operation of networks and the causes of faults must be identified in (almost) real time. Regular and cost-efficient inventories must be performed on the state of devices connected to the networks (the objects to be secured). Network overload must be pre-emptively prevented through continuous monitoring. Any cybersecurity breaches and data leaks in the networks must be identified.

Production, network, asset and capacity monitoring must all be comprehensively targeted during technical monitoring of the cybersecurity state.

Monitoring networks in a production unit

Cybersecurity controls and monitoring of the status of cybersecurity should be tailored for and integrated with the production unit during the design phase. This will avoid the need to add expensive cybersecurity solutions afterwards, which may change the architecture.

Using the services of a single automation system vendor seldom results in successful threat monitoring, since the environment is almost always multi-vendor. Automation vendors also have their own service limitations regarding support for old products or platforms and due to the pressure to introduce new products.

The orderer must understand requirements related to the cybersecurity of the production unit and the development of such requirements throughout the lifecycle. Specialists should be consulted to determine the events that need to be logged. Important principles include the strong protection of log entries so that no one can modify them. In addition, it must be ensured that log entries cannot fill up the memory, jamming the machine. In the case of complex log entries, a professional log analysis should be ordered regularly if internal competencies do not suffice.

In industrial automation in particular, instructions that force simplicity and a clear division of tasks should be adhered to:

1. Do not add separate information security software to the intelligent device.
2. Use the device's own protection, storage and log procedures, for example information security procedures in Windows.
3. If separate information security system is added, its management and use must be separated from the rest of the equipment because it will introduce new vulnerabilities and attack vectors of its own.

Following trends

Monitoring the state of cybersecurity can be supported by monitoring change trends in various systems. For example, the development of indicators or weak signals related to the realisation of threats to the company's production networks and systems.

Examples of trend monitoring:

- UPDATES: Number and availability of patches and updates, installation success.
- VULNERABILITIES: Number of vulnerabilities and applicability to the company's systems.
- PERFORMANCE: Changes in the availability and performance of systems.
- DATABASES: Database queries and register changes.
- FILES: Unexpected changes to files.
- RECONNAISSANCE: Unexpected queries to subnets (e.g., using Honeynets).
- ACCOUNTS: Unexpected changes to user accounts.
- PROFILES: Unexpected changes to user profiles.

Changes in trends enable the more precise cybersecurity monitoring of suspicious objects.

Trend monitoring should be integrated with broader operational monitoring, in which anomalous activity stands out from normal activity mass by exceeding the thresholds for "normal." Detailed trends can easily be monitored, including graphically, using customisable indicators based on commercial and open source code tools.

Evaluation of monitoring services

The applicability and capacity of external monitoring services should be evaluated. A service evaluation of this kind is needed, for example, by parties responsible for monitoring the cybersecurity of an internal network at a production unit.

The test programme can include the following steps:

- network scanning
- downloading files from an external network
- Netcat scanning
- starting the Tor network (for test purposes)
- encrypted exit path for data
- new IP address in the network
- atypical TCP traffic

Securing embedded systems

Persons responsible for the procurement of automation systems, machines and devices must have a strong understanding of the impact of production automation solutions on security.

The physical data network architecture consists of physical switching devices (switches, gateways, base stations, routers, bus controllers, firewalls), buses and cables whose protection requires physical access control. Previously, the network architecture strongly differentiated between fixed automation and safety buses, separate building automation networks and local area networks (LAN and Wi-Fi). Networks are now evolving and converging, resulting in new technology choices. Maintenance of wired networks in industry and buildings deteriorates over time; rectifying this situation requires updates and creates an opportunity for technology rethinking.

A logical data network architecture is based on logical, often functional, levels of shared areas with tight restrictions on the traffic between them, such as firewall rules, filtering rules and virtual subnet definitions. Key problems involving logical network architectures include the gradual degradation of firewall and filtering rules and insufficient cybersecurity testing. The target level of the cybersecurity set by the company determines the scope and depth of isolation of data networks. The key issue is that each network can be credibly maintained and monitored during all stages of the lifecycle, in accordance with the specified level of criticality. The measures taken by a company's own personnel are insufficient for sustainable monitoring throughout the lifecycle, since production network technologies and automation applications with competing ecosystems are developing rapidly, and cyber threats are increasing.

The implementation architecture of an intelligent device, including the embedded computing and system platform of the controller board, can be a highly complex entity which includes several protection technologies provided by an advanced platform. Protective technologies are not being fully used or implemented, because the existing security methods are not always switched on. The reasons for this may be lack of expertise and experience, or lack of test opportunities and time.

Several security techniques exist, such as access control to various areas of memory, access control to I/O interfaces and peripherals, system start-up process monitoring, access control for and disabling of debugging interfaces, an internal operating system and all of its security features and settings, and prevention and monitoring mechanisms for application installation and start-up.

Although secure implementation of the architecture and applications of an intelligent device is usually the responsibility of the device developer and manufacturer, integration as part of the whole is an important stage. The manufacturer should also be able to support the integrator company in relation to information-security-related issues and choices.

Virtualisation

Use of virtualisation is here to stay, including in automation. It allows the limitation of threats due to the vulnerabilities of outdated and non-updated systems, for example. An obvious downside is the fact that it is accompanied by IT-based virtual platforms and systems with their raising competence requirements. Virtual environments can, however, also be used to reduce complexity.

Cybersecurity exercises

A cybersecurity exercise arranged by an outside party has become an important way of developing security awareness within businesses.

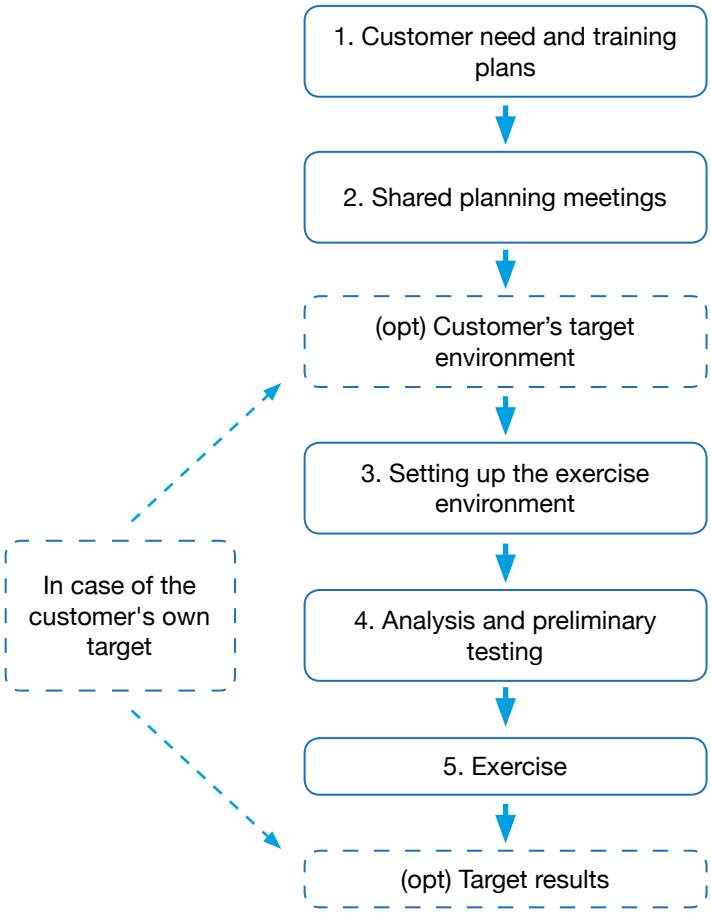
Cyber exercising can be implemented through a participative workshop, for instance, in which the participants' cybersecurity awareness and competence are developed.

Practical exercises provide the participants with the capacity to critically examine their own behaviour and the company's practices:

- Do I pay sufficient attention to security in my work and private life?
- Could my private life, for example in relation to the social media, affect the security of my work?
- Have the production devices I use or administer been exposed to cybersecurity threats?
- Does my company have sufficient backup arrangements in production and do they work?
- Do we practise our methods of preparing for anomalies?

Exercises according to the needs of the company

The planning meeting should involve a discussion of the development goals of cyber-security, potential shortcomings in the competencies of key persons and training plans, as well as information security instructions.



Model of the design and implementation of a cyber exercise.

The most efficient method involves cybersecurity experts targeting and pre-analysing vulnerabilities or other serious problems in the customer's own systems. The easiest way of achieving this is for the customer to assemble the target system selected for the exercise and confidentially deliver it to the exercise's implementer for pre-analysis. In the actual exercise, developers and maintenance personnel are instructed to try out the applicable testing tools, and practise the identification of a cyberattack and the applicable protection measures.

Workshops as a thought-provoking motivator

A cybersecurity workshop motivates its participants to give thought to the protection of their own automation system against cyber threats and encourages the development of processes and methods used for identifying attacks. Participants receive first-hand information on various cybersecurity requirements, methods and tools and are encouraged to consider the importance of teamwork and sharing experiences.

In addition, understanding the attitude of the attacker and the nature of the available concrete tools plays a key role in providing the participants with a realistic understanding of the opportunities and attack vectors of the attacker.

Summary

As the level of automation increases in industrial environments, information networks and systems are being exposed to a range of cyber threats and attacks.

Even an unintentional disturbance can cause damage worth millions: loss of production, broken equipment, contaminated environment and personal injuries, for example. Efficient protection against cyber threats is critical.

Typical challenges of the kind presented in our report help to identify the areas worth investing in during development of cybersecurity. The solution proposals we present are supplementary, rather than being mutually exclusive.

Because so many variables are in play, the cybersecurity situation is different in each organisation. There is therefore no single solution that covers all aspects of protection, but best practices must be applied to developing and deploying company-specific security plans.

If you need more information or want to discuss how we can help your company in the field of cybersecurity, contact:

Pasi Ahonen
Principal Scientist, VTT Ltd
Tel. +358 20 722 2307
E-mail firstname.lastname@vtt.fi.

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD
P.O. Box 1000, FI-02044 VTT, Finland
Tel. operator +358 20 722 111
www.vtt.fi