ADDRESSING THE CHALLENGE OF CYBER SECURITY MAINTENANCE THROUGH PATCH MANAGEMENT

Adam GAUCI
Schneider Electric – Canada
adam.gauci@schneider-electric.com

Sebastien MICHELIN
Schneider Electric – France
sebastien.michelin@schneider-electric.com

Mathieu SALLES
Schneider Electric – France
mathieu.salles@schneider-electric.com

ABSTRACT

In December 2015, a confirmed cyber-attack targeting several electric power utilities in Eastern Europe has resulted in a power outage that impacted hundreds of thousands of utility customers[1]. This event strongly indicates that DSO systems are vulnerable and are high risk of being targeted.

With the plethora of new connected components inside the DSO's systems and readily available vulnerability information available on the Internet, there is a greater risk of outages due do compromise caused by a cyber-attack.

To help reduce risk and potential cyber-attack surface, DSOs must implement a security organization and adopt active security processes. This paper will describe one of those processes that must be actively maintained.

Mitigating risk and anticipating vulnerabilities on utility grids is not just about installing once at the latest technology. DSOs must also pay special attention to implement regular or routine maintenance of equipment which includes patch management and necessary security updates in the system.

DSOs are today facing difficulties to deploy an efficient patch management programme.

A suggested methodology and a smart patch management system based on IEC62443-2-4 standard will be discussed, comprising:

- *A process for vulnerability detection,*
- *A tool to automatically assess DSO system components,*
- *A corrective patch implementation recommendation.*

The final update decision is made on a regular basis and in a selective way by the DSO security administration team.

.INTRODUCTION

Cyber security is about people, processes, and technology, in exactly that order. DSOs need to deploy a complete programme consisting of proper organization, processes, and procedures in order to fully take advantage of cybersecurity protection technologies.

Developing competencies and cross-functional teams for OT and IT integration becomes key for DSOs to address the unique challenge of securing their modern control systems.

OT – Operational technology is related to the real-time operation of the electric grid, it needs to ensure high reliability and availability.

IT- Information Technology is related to PC/Server control rooms

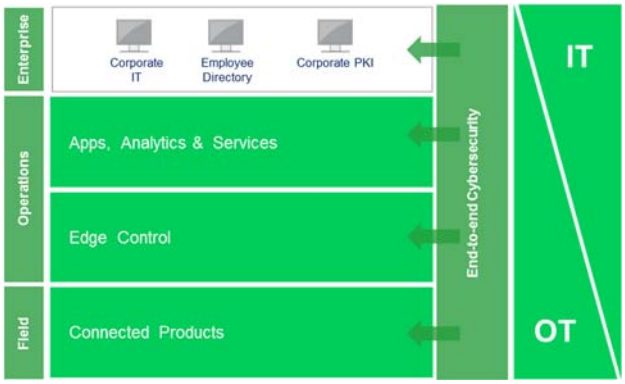


Figure 1: OT/IT cyber security integration across the DSO system.

Energy industry standards and guidelines, such as for instance IEC62351, or IEC62443 are great tools to define a good level of security. Many European vendors have harmonized their operations and internal processes to align with these international standards[2]. So cyber security is not only a matter of having 'achieved' a cybersecure state. Adequate protection from cyber threats requires a thoughtful, thorough, and ongoing analysis of many variables as well as an iterative vulnerability management process.

So it is important for DSOs to think about how their cybersecurity strategies will evolve over time. This is about making the DSO system more secure and ready to protect the system from possible known threats in a planned and iterative manner. Ensuring a strong defense against cyberattacks requires a continuous effort.

Therefore, DSOs need to understand the uncertain risk by quantifying it in an initial cyber security assessment, comprising below:

- Inventory of critical cyber assets within systems, regardless of vendor,
- Identification of threats and vulnerabilities related to

these assets,

- Identification of the associated risk level,
- Definition of an action plan of mitigating measures,
- Implementation of mitigating measures,
- Definition of a process aiming to manage and maintain the security level.

PATCH MANAGEMENT SYSTEM: WHAT ARE THE MAIN IMPLEMENTATION BARRIERS?

Managing the lifecycle of all software-based assets (embedded devices, network infrastructures, host based systems) implies to have the full knowledge of their components, applications or operating systems. Every day, corrective patches, impacting both functionalities and security are likely to be published.

The patch management system establishes processes and tools aiming to efficiently drive the user in implementing those patches and overcome the today existing pain points and threats related to cyber-attack.

In this paper, only the security patch management is addressed.

Pain point #1: how end user detects that a new patch is available for upload or upgrade?

End users have several possibilities to access to vulnerability information:

- **Passive**: end user is directly notified by the vendor, via a direct communication or a subscription to a notification service.
- **Active:** vendors usually publish the vulnerabilities of their products and the end user can access to this publication. For example, Schneider Electric is updating a dedicated web-page.

Vulnerability and associated corrective patch shall be properly identified and documented. The IEC62443 standard defines a set of identification and documentation information that can be classified into three categories:

1. Vulnerability information
2. Corrective patch information
3. Impacted vendor product patch information

Vulnerability information

- Product description: it is a software sub-component used into the commercial product (e.g. Operating System, communication driver, SGBD, …)
- Reporting date & Vulnerability Id

The vulnerability is generally concerning a software component that is used within the vendor product firmware. This implies that the vendor shall document each and every component and put in place an efficient surveillance process in order to properly follow-up and trace all the vulnerabilities it is exposed to.

Corrective patch information

- Patch date : patch publication date
- Patch version

The corrective patch is associated to the vulnerability. Because of the existence of a profusion of patches, it is essential that the relation with the eliminated vulnerability is unambiguously documented.

Impacted vendor product patch information

- Vendor patch product (e.g. IED)
- Vendor patch product date
- Vendor product line version
- Vendor patch product version
- Release date
- Applicability
- Test result
- Mitigation
- Patch implementation recommendation (possible impact)
- Associated risk

For the end user perspective, this is the most crucial point to be managed. Indeed, within a DSO system, the “vendor products” are the ones which are directly linked to the electrical process. These products are:

- Embedded Devices: gateways, controllers, RTUs, protection devices, measurement & metering units
- PC hosts: Windows PCs, Linux PCs
- PC-based applications: software such as local Human Machine Interface, engineering tools (configuration, maintenance, settings)
- Network infrastructure: media converters, Ethernet switches, routers, firewall, time synchronization devices.

A vulnerability addresses a sub-component, impacts one or several vendor products, making the process of detection and identification more complex.

Pain point #2: which patch is applicable to my system?

Fortunately, vendor products are not affected by all the notified vulnerabilities. Vendors are publishing the list of vulnerabilities, their details, the associated

corrective patch and possibly the recommendation on their affected products.

End users shall cross-check with their product installed base in order to confirm that they are impacted by the notification. A specific attention shall be paid on the identification of the product name, the product number, eventually the serial number, the vendor product firmware version.

This means that end users shall put in place a dedicated process to make a full inventory of their system electronic devices, and maintain it as always up to date.

Then end users shall proceed to the implementation risk assessment. They shall have a clear statement on the impact of the corrective patch installation for their runtime application context.

As a conclusion of this point, impacted products shall be unambiguously identified, the end user shall always have the exact visibility of its installed base and the associated implementation risk shall be properly assessed.

Pain point #3: Patch needs to be tested in a non-production environment

When vulnerability is confirmed for one given vendor product, the corrective patch implementation process shall be initiated.

A direct implementation on the product may affect the end user process and could result in an uncontrolled downtime. It is then important to test the patch and determine if the system will continue to behave normally and if no collateral effect will cause a system partial or complete failure. Indeed, within DSO systems, there are existing interactions between system devices, necessary to achieve the end user specified functionalities (distributed automatic scheme, inter-tripping, inter-locking, etc…).

This implies that end users shall have an access to a mirror testing platform that hosts each and every product they own. Moreover, this testing platform shall be configured with their runtime application in order to make sure that no unexpected failure, linked to the application implementation will occur. This testing facility can either be located in-house or can be part of a supporting service offered by a vendor.

This test on non-production environment is an effective method to confirm the patch implementation risk assessment.

Pain point #4: How to properly apply the patch?

The last mile to run is the site implementation. End users shall train and certify their staff for the site intervention and implementation.

The patch installation procedure shall be rigorously executed, on the correct set of products. A corrective patch that is not properly installed, or installed on the wrong product, or a procedure that is not fully executed up to the last step can make the patch ineffective. The end user could be in a situation where he thinks security is under control whereas the vulnerability is still present on the system.

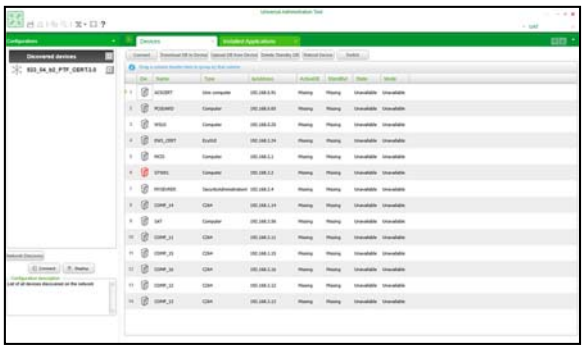
Another important point to be considered for the end user is the intervention planning. Will it require a system partial shutdown? Will it require a process partial downtime? What will be the impact on the end user business? This question is legitimate when for instance the patch implementation will target a protection relay, or a controller. This equipment is directly connected to the circuit-breakers commands and can at any time perform an open command.

To summarize this point, only certified people can identify the products and properly execute the installation; the intervention shall be properly planned in order to minimize the possible downtime period impacts.

HOW CAN PATCH MANAGEMENT BE MADE EASY?

System inventory management

System inventory provides the capability of scanning all connected electronic assets, possibly installed in different segments of the DSO system. The result is the list of assets with a set of properties such as for instance network name, IP address, firmware version, manufacturer name, product name, etc.



In addition, for each single product, the system inventory brings visibility on all applications that are installed, their version, their editon and their installation date.

Security bulletin

The security bulletin is the list of identified vulnerabilities on all assets connected to the systems. This includes (not exhaustively) operating systems, device firmware, drivers, or application software. It follows the IEC62443-2-3 recommendation for patch management.

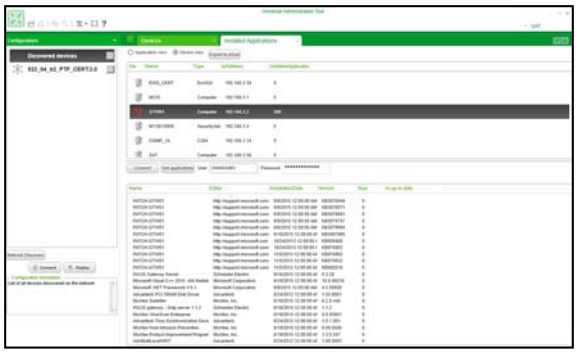
The security bulletin is the result of vendor cyber security expert analysis of announcements regularly

published by product vendors.

The security bulletin is regularly updated and can be distributed to the end users using a safe repository.

Patch management baseline

The patch management baseline is the outcome of the system inventory, combined with the security bulletin. In details, after executing the inventory scan, the security bulletin is imported within the tool. Then a comparison between the previous baseline and the most recent bulletin is computed. The results help to highlight the gap between the current installation and the vendor security recommendation.

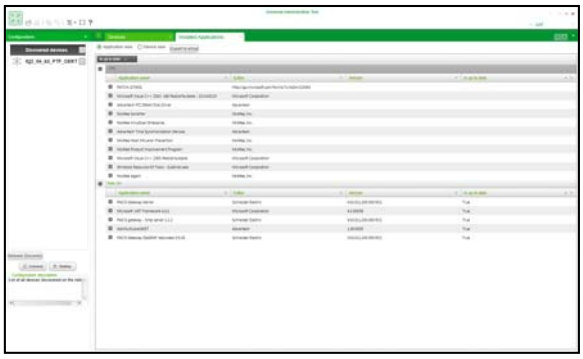


A dedicated service allows the tool to retrieve the most up to date security bulletin from the safe repository. This guarantees that the assessment has been done on the most recent vulnerabilities list.

Vulnerability risk assessment

The security bulletin also provides with the vulnerability associated risk, at the vendor product level. It informs about the impacts of the vulnerability on the products that is helpful information for the end user to properly assess and rank the associated risk.

This information is accessible inside the tool for each highlighted gap.



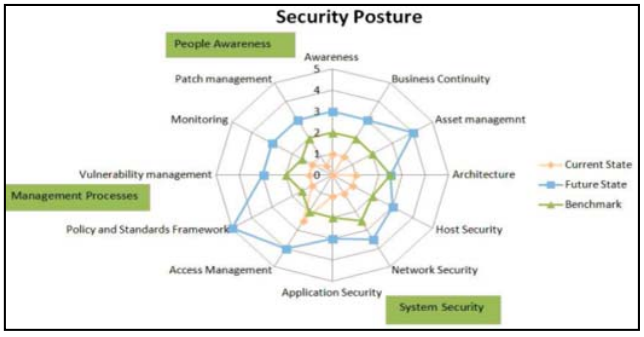
The final update decision is made by the DSO security administration team based on this information, taking into account the company rules and planning.

CONCLUSION: SOLUTION BENEFITS

DSOs have structured their approach and raised recommendations for implementation. Their security assessments lead to build Cyber Security Heat-Maps to identify and classify the areas of improvement as per industrial standard domains.

With the solution described in this paper, DSOs get a structured assessment and corrective method to:

- Enter into a virtuous security circle and progressively move from uncontrolled security state to more controlled security state.
- Optimize the electronic critical assets life-cycle management and move to supported and secured versions of components
- Feed the cyber security heat-map for the exposure of each asset to cyber-security risks.



The technical solution, Operation Technology oriented, is vendor agnostic and offers the required openness to evolve in the DSOs eco-system. It efficiently participates to tackle the main pain points linked to the patch management solution implementation.

REFERENCES

[1] Robert Lee, 2016, "Analysis of the Cyber Attack on the Ukrainian Power Grid", *https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf*

[2] T&D Europe, 2016, "Harmonized Cyber Security Standards for the European Union Electric Grid Position Paper", *http://www.tdeurope.eu/data/TD%20Europe%20-%20Position%20Cyber%20Security_291116.pdf*.