How to use cyberattacks to increase security

A cybercriminal can resist anything except temptation

In order to systematically detect and defend against hacker attacks on industrial targets, so-called honeypots scenarios are often used. In many of these, false pots of honey are left out in the open and the real pots of honey—valuable data, software and hardware—are protected as a result. A good example of a false pot of honey in an industrial environment is a data-routing network switch. In this article, we take a closer look at how this could theoretically work in an operational production facility.

If we want to effectively protect ourselves at the earliest possible stage against attacks, we need to understand the continually evolving strategies being used by hackers. Obviously it is not a simple matter of disabling the firewall and password-protection then waiting to see what happens. You would certainly experience a wave of attacks, but would learn little or nothing about real-world sophisticated attempts to steal and manipulate. And, of course, it is completely out of the question to expose real data, which in many cases would not only be irresponsible, but also illegal. But there are ways of using honeypot scenarios to open the door, just a crack, without risking damage. No company, however, should ever attempt to do so without first obtaining expert

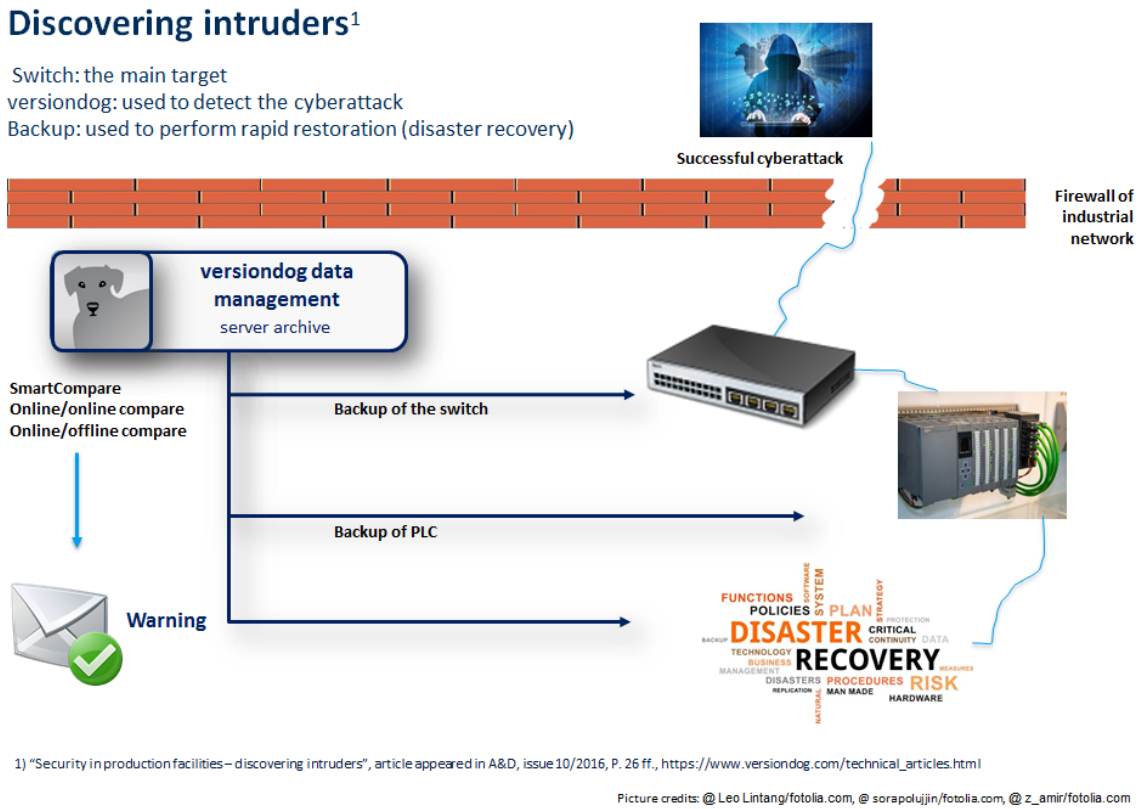

Fig. 1: Classic honeypot scenario: A "dummy" switch is set up to attract attacks then closely monitored

guidance. Anyone interested in the honeypot scenario described in this article should develop it in consultation with their company IT department and advisors. Only they will be able to confirm that there is no additional risk to data or hardware and that no liabilities are incurred. Liability for damage or loss resulting from any action that increases risk is typically borne by the person who took the action.

Allowing a cyberattack

In the industrial environment—and especially in critical infrastructures (CRITIS)—cybersecurity has become an extremely high priority. In this context, anything that can be done to warn of hacker activity and/or learn about hacker tactics is worth considering. So if, paradoxical though it may seem, we have decided to allow a cyberattack as a defensive strategy, where could we start? Automated environments typically have numerous controllers, robots, drives, HMIs etc. connected to a network. Network switches are used to connect components to the server, monitor data traffic and route it to where it is needed. Their data-routing functions, together with their access management functions make switches a classic target for cyberattacks, and, as such, the ideal honeypot.

A switch as a honeypot

Network switches perform essential functions in connecting robots, drives, PLCs and other devices to the industrial network. As a result, their firmware and configuration are vitally important and should be well-protected:

- Switch firmware is, similarly to operating systems, subject to manufacturer modifications and updates.
- The configuration of a switch encompasses a range of settings including which ports are used for which data traffic flowing to and from which connected devices.

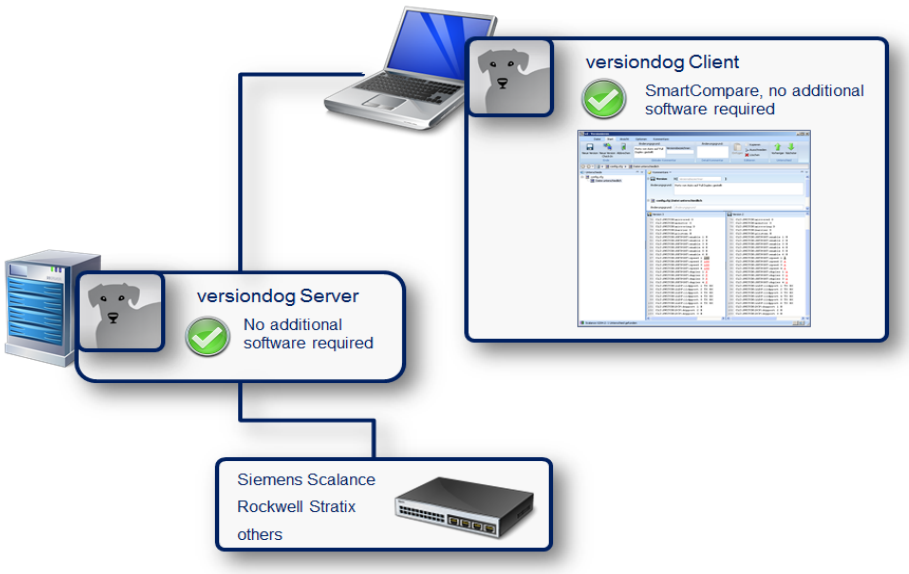

Fig. 2: Switch management with the data management system versiondog

Attackers who want to do damage within a network can manipulate the network communication of a switch. Switches are often used by hackers to establish a connection with a component, e.g. by opening and closing ports. In this way, erroneous data can be routed.

Being a favourite targets of hackers is what makes network switches so suitable as honeypots. One scenario involves installing a superfluous switch in the industrial network. This switch is set up to look attractive, but, as it has no real function, it can be completely left alone by company staff, all of whom are informed of its actual purpose. With no changes at all being made internally, any changes that are made to the switch must have been made by an unauthorised external party.

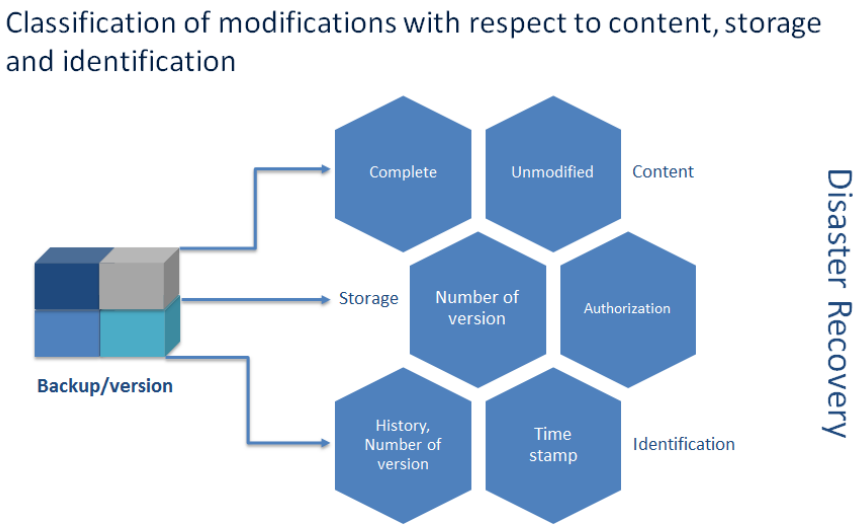

Fig. 3: How data backups/versions are classified according to content, storage and identifier in order to facilitate fast disaster recovery in production

The trick is to detect these changes as quickly as possible. This is where a data management system can be used. But this system will need to have the capability to regularly and automatically check the state of the switch, detect even the smallest change, then alert the appropriate personnel without delay. Any manipulation might be an attack in itself, or it could be the preparation for an attack. Either way, early warning will help avoid damage or loss, and detailed inspection of the changes will reveal the tactics being used.

A data management system

versiondog is a data management system that is installed on computers connected to the industrial network of a manufacturing or CRITIS facility in order to manage change and safeguard data. It easily fulfils the criteria required by this honeypot scenario with its backup and compare functions. While it does not replace other network security measures, such as firewalls IDS systems and IPS systems, it can be used alongside them as a valuable extra layer of security. This is because it can be set to automatically and precisely compare current device data to previous device data at regular intervals. For the network switch in our honeypot scenario, the focus will be on ports, which could allow a hacker to gain access to automation equipment and potentially wreak havoc.

Together with a disciplined version control system that includes clear and complete documentation (**who changed what, where, when and why**), versiondog's automatic backup and compare functions are important components of an effective cybersecurity strategy. Each new backup is compared with the previous backup, and in the case of our honeypot switch, nothing should have changed. If a change is found, the system administrator is alerted and can take the appropriate action. And if the worst comes to the worst and disaster recovery is necessary, the last non-manipulated version of any device data or control program can be located and restored quickly and with confidence.

Cyberattacks on industrial facilities and public utilities have, unfortunately, become a reality. Because of the complexity of these largely automated environments, only a multi-layered approach can effectively protect against potentially serious losses. As part of this defence in depth strategy, honeypot scenarios such as this are one component of many – a little more safety, certainty and security for us and the environment.

www.versiondog.de

Author:
Dr. Thorsten Sögding
Head of Business Development
AUVESY GmbH
76829 Landau in der Pfalz
Tel. +49 6341 6810-560
Thorsten.Soegding@auvesy.de

Co-author:
Stefan Schnackertz
Business Development
AUVESY GmbH
76829 Landau in der Pfalz
Tel. +49 6341 6810-442
Stefan.Schnackertz@auvesy.de