secXtreme White Paper

IT security in production environments (SCADA[1]) honeyBox® versus Stuxnet

Stuxnet is the first high-risk potential malware known to have attacked production environments. Classic IT security failed to protect against it. Had the honeyBox® Honeypot Appliance been installed in the sites that were attacked it is highly likely that Stuxnet would have been detected upon initial infection, long before it was discovered in mid-2010.

1 Abstract

This White Paper describes the problems with IT security in industrial applications and the differences between the IT used in offices and in production areas. It outlines the IT security measures used to protect classic IT assets. It explains the requirements regarding security components in process IT and how, whereas classic approaches are totally ineffectual in industrial applications, these requirements can be addressed by installing the honeyBox® Honeypot Appliance.

2 Background

Automation and control technology has up to now been characterised by systems that communicate with each other using dedicated technologies and protocols. These include, for example, the RS-485 interface, PROFIBUS and CAN Bus. Planning and programming of plant is normally accomplished using software on separate PCs in Production.

But the ubiquitous network technology based on ethernet and TCP/IP is increasingly gaining ground in such environments. First of all the PC stations are linked up and after that the instrumentation and control technology. More and more programmable logic controllers (PLC) are being connected to the LAN while compact controllers based on embedded systems are increasingly offered with LAN interfaces.

As an established communication path, TCP/IP on ethernet is increasingly advancing into what were previously "TCP/IP-free" areas of production and control technology. Industrial Ethernet has arrived on the market and is now offered by a number of product manufacturers. Even WLAN components have meanwhile matured in line with the harsh requirements of production environments and are in use there.

As a result, data communication in the office and internet areas on the one hand and production facilities on the other are increasingly merging. This allows some synergies. In this context it is essential that process data can be visually represented and analysed. In the energy area,

[1] Supervisory Control and Data Acquisition

generation and consumption data has to also be instantly exchanged between energy suppliers.

3 Adequate security must be guaranteed

In industrial environments the emphasis tends to be on safety, as in failsafe operation, electrical safety, safety for operating personnel, protection against environmental influences and explosion prevention, rather than on security.

The security risks that are typical of internet and office activities, such as denial-of-service attacks, the manipulation of data and systems, data snooping and system penetration, often go unmentioned, undetected and to all intents and purposes ignored. In the past there was no need to do otherwise.

4 Security problems

The introduction of ethernet and TCP/IP to production environments creates new security problems there that previously did not exist. Moreover, the linking of process networks to the office world or even to the internet is leading to new and significant risks.

4.1 Problems caused by the use of ethernet and TCP/IP

Ethernet and TCP/IP offer hackers or malicious software a standard dissemination path. Less and less specific information is required about the plant, enabling standardised attacks (e.g. Stuxnet) to succeed.

Existing and new implementations of TCP/IP protocols in equipment are flawed. These shortcomings may also be important from the point of view of security.

4.2 Danger from interconnection

Now that the office and internet areas are connected to the production and process networks, suddenly all the threats from the former are now present in the latter. A secure enclave has overnight been transformed into part of the global village. Recognising this, assessing the risks and taking the appropriate action may well be beyond the capabilities of the staff responsible for the process IT, with their limited security expertise.

On the other hand in the office area where classic IT security solutions prevail, there is little understanding of process IT and its sequences of operations, requirements and protocols.

The question then frequently arises as to who is responsible for IT security and who possesses the necessary expertise. In our experience the only way to ensure a proactive approach is for the two different areas to work together. Process IT staff have to get to grips with the threats from the office world with which they are as yet unfamiliar. At the same time the staff who manage the office IT need to build up expertise in the process IT area. This convergence not infrequently results in areas that were previously organisationally separate growing closer and closer together after a certain time.

4.3 Possible solutions with known procedures from the office world

To neutralise the new threats in process IT, usually the only IT security measures considered have their origins in the office world. These include:

- patch management
- virus protection
- firewalls
- intrusion prevention systems (IPS)
- However, these solutions are at best of only limited suitability for process IT and may in fact be totally unsuitable. There may be following reasons:
- Operation presupposes a high degree of expertise in IT security, especially in the case of intrusion prevention systems. This expertise will initially be absent in process IT and therefore has to be built up.
- Operation of these solutions is very time-consuming. IPS in particular requires constant maintenance to ensure secure operation. Again, the virus protection software should as a minimum incorporate the very latest virus signatures, on every system. The technical realities frequently rule out the online distribution of patterns. Updating systems from the internet itself is highly problematic from a security point of view, so that often manual procedures are the only option.
- A lot of process IT systems are tested and accepted as they are. This often prevents the installation of patches or virus protection software.
- The pre-eminent classic IT security goal of process IT - availability - is significantly impaired by the use of firewalls and IPS. Both approaches require that data traffic passes through these systems. But this only creates new risks of disruption. Moreover, these systems are designed to deliberately block traffic (IPS) or to only permit traffic relations that have been manually allowed (firewall). IPS updates can result in the situation where traffic that flowed in the proper manner before an update is blocked afterwards. This implies significant risks to the availability of the process networks.

In this way, the application of classic IT security measures to process IT can lead to new problems, with the risks outweighing the benefits.

Such approaches (firewall, IPS) do make sense at the point where data passes between the office network and the process network. But other concepts are required inside process networks.

5 Requirements for process oriented IT-security solutions

In our view IT security solutions in process IT must satisfy the following requirements:

- No adverse impact on availability
- No increase in the complexity of the network (e.g. as a result of high availability protocols)
- Little installation effort required
- Inexpensive to operate

- No false alarms
- Ability to link alarms to graphical representation of processes
- Simple and comprehensible alarms that the layman can understand
- Hardware suitable for an industrial environment (environmental conditions, mounting rail assembly, power supply)
- Low unit price

6 Solution with honeyBox®

6.1 Operating principle

honeyBox® operates by making virtual sacrificial systems (honeypots) available in process LANs so as to attract attacks towards them. At the initial stages of an attack (manual or automatic investigation of LANs, scans etc.) hackers and malicious code (e.g. Stuxnet) then encounter real systems and virtual honeypots. As far as the hacker is concerned, initially these are indistinguishable from the real systems but are in a poorer security state. In subsequent phases of an attack the honeypots direct the further activities of the hacker or malicious code onto themselves. An alarm is raised at the very first contact with a virtual honeypot.

6.2 Fulfillment of requirements in an industrial environment

The honeyBox® Honeypot Appliance from secXtreme satisfies all of the requirements listed in section 5 above, namely:

Availability: honeyBox® is connected to a switch like a normal terminal device. Traffic is not passed through the device. If honeyBox® fails, production data continues to flow.

No increase in the complexity of the network: honeyBox® is connected to a switch like a simple terminal device. It behaves purely passively during normal operation.

Little installation effort required: For a standard configuration it takes just half an hour to configure honeyBox®. If there are multiple devices, configuration can be automated. The only installation work required on site is to install it in the mounting rail, connect the power supply and plug in the LAN cable.

Low maintenance and operating requirements: With honeyBox® there is no need to load new patterns and signatures. All that is required is to install security patches at regular intervals. As honeyBox® has a high degree of self-protection, this is only necessary instantly in certain environments. Moreover, installation of updates can be automated. Every honeyBox® monitors itself and autonomously corrects a number of fault conditions.

Low false alarm rate: honeyBox® does not sound an alarm unless an attack has actually taken place in the network. The quality of the alarm signalling is therefore very high.

Ability to link alarms to graphical representation of processes: honeyBox® industrial offers optional digital outputs that can be connected to the process control system. In this way an attack can also be presented in the process visual display system and IT security becomes an integral element of the process.

Simple and comprehensible reports: Alarms issued by honeyBox® can be readily understood even by staff without expertise in IT security. They indicate what happened where (e.g. attack on an FTP server of a virtual honeypot with attempted log-in), rather than the information that "vulnerability XY with number CVE-yz has been exploited". In this way the messages can be understood by anyone with a general IT knowledge.

Hardware that is suitable for industrial environments: honeyBox® industrial is designed for use in industrial environments. It can be operated over a wide range of temperatures. Even the Flash card used is an industrial design. Moreover, the system does not contain any moving parts. honeyBox® industrial is designed to be installed on mounting rails. The power is connected via a DC input. No keyboard or screen are necessary for operation or service. Local access is via a serial RS232 port.

Low-cost: honeyBox® industrial is costed in such a way that even if when used at multiple points in production, it is still cheaper than classic IPS systems. It is therefore possible to use a large number of systems at lower cost and with wider coverage.

7 honeyBox® in practice

honeyBox® won the Bavarian Security Award 2009. It was shortlisted for the IT Mittelstand Innovation Award in 2009 and 2010. The solution is already in service with many customers where it has more than demonstrated its worth.

8 Further links

- honeyBox® data sheet, http://www.sec-xtreme.com/fileadmin/download/public/secXtreme_honeybox_honeypot_appliance_rel5_0_en.pdf
- Stuxnet, Wikipedia, http://en.wikipedia.org/wiki/Stuxnet
- All about Stuxnet, http://www.stuxnet.net

9 About the Author

Christian M. Scheucher has been working in IT security for many years. He has implemented many solutions for the detection of attacks. In the context of the IT forensics services offered by secXtreme, he detects attacks and tests system security using penetration testing. honeyBox® is his brainchild.

10 About secXtreme

secXtreme GmbH is a company that is specialised in IT security consultancy and services. secXtreme offers intrusion detection and tracking services, (web) application security and audits. secXtreme also develops Linux-based security solutions for specialised IT security requirements secXtreme is a member of the German Computer Emergency Response Team (CERT) Network.

Contact information:

secXtreme GmbH
Kiefernstraße 38
85649 Brunnthal-Hofolding

Tel. +49 (0)89 – 18 90 80 68 -0
Fax + 49 (0)89- 18 90 80 68 -77
E-Mail: info@sec-xtreme.com
Web: http://www.sec-xtreme.com