Perimeter Protection

Introduction

In late 2014, a steel mill in Germany suffered massive damage as the result of a cyber attack that required advanced hacking skills, applied industrial control knowledge and endurance. No one has claimed responsibility for the attack and the lack of attribution and clear objective emphasize that not only are the threats very real, but anyone can become a target without apparent reason. This incident is only one of many examples of successful cyber attacks of industrial automation and control systems, and together with Stuxnet manifests the reality of cyber threats.

Unless you have experienced a serious security incident first hand, it is easy to believe such attacks only happens to someone else, but not having experienced such an incident however, does not mean you haven't been compromised. In fact, according to a report from KPMG from 2014, it is more likely than not that information is being exfiltrated by malware without your knowledge from your office networks. 14 companies were studied, and data was actively stolen from 10 of them without their knowledge.

The report is yet another strong indication traditional, best-practice defense like anti-virus, perimeter firewalls and network intrusion detection systems based on signatures are easily avoided. It also indicates insufficient organizational readiness as no action was taken even when malicious code was detected.

Westermo present a series of five basic applications assets owners can apply in their own networks to improve the security posture in a sustainable way.

Perimeter Protection

One of the most common components in a security program is identifying and protecting the outer logical and physical boundaries of an organizational location. There are different physical access controls to ensure only authorized personnel can enter, for example using keypads, key and miscellaneous other tokens. Similarly, there is a firewall connecting the local networks with an external network like Internet for office networks, or the office network if the local network is an industrial automation and control system (IACS).

As the name implies, these controls are called perimeter protection or perimeter defense simply because they create physical and logical shells that protects the sensitive inside.

This security control is usually reasonably easy to implement in most organizations as there should be a very limited set of data exchanged through the boundary, and therefore reduces the external

network based attack surface enough to filter out the background noise, for example automated probes and attack attempts originating from the Internet or an infection in the external network.

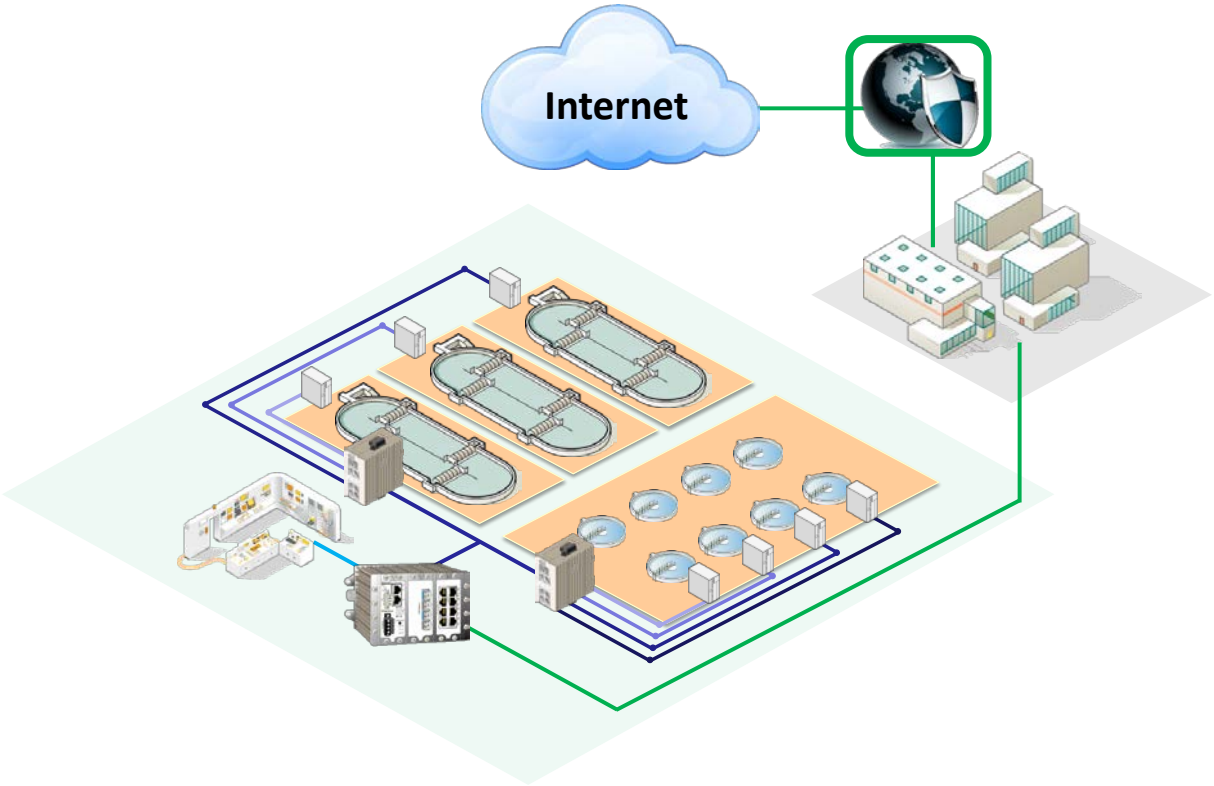

Figure 1 – Typical Perimeter Protection

Protection

The classic application is to protect all assets on the office network from external connection requests. Assets that should be accessible from the Internet such as web and email servers are placed in a separate network, often called DMZ. All connection requests to assets in the office or control networks originating from the Internet or DMZ are blocked. Email clients on the office network and sometimes control network then connect to the email server in the DMZ to send and receive new emails.

Considering the huge amount of unsolicited connection requests from the Internet, it is often impractical to log everything that is dropped, it is simply too much noise. Logging requests from the DMZ to the office networks however another matter as that is probably shouldn't happen to begin with.

However, the purpose of a logical shell that a perimeter firewall constitutes to protect all assets within is commonly defeated today with watering hole and drive by attacks, where the attacker

poisons resources on the Internet or the DMZ (like e-mail) that people on the trusted network accesses with their web browsers or e-mail clients. With this very successful attack, the perimeter firewall is simply bypassed as people on the inside access the contaminated resources directly themselves.

Detection

As infections are actually brought to the inside by people on the inside, it is important that the perimeter protection device also protect and monitor outgoing traffic (egress). In an office environment where employees are used to being able to access the Internet more or less freely, controlling the outgoing traffic is difficult.

In closed environments, like an industrial control system where data flows are known and static, it is relatively easy to control and monitor data exchanged at the boundary, and WeOS devices becomes a valuable addition to the intrusion detection architecture.

Typical application

Appreciating WeOS are of greatest value in environments where data flows as known and static, especially traffic through the perimeter boundary, we should target industrial networks as illustrated in *Figure 2 - WeOS Target for Perimeter Protection*, rather than enterprise network perimeters.

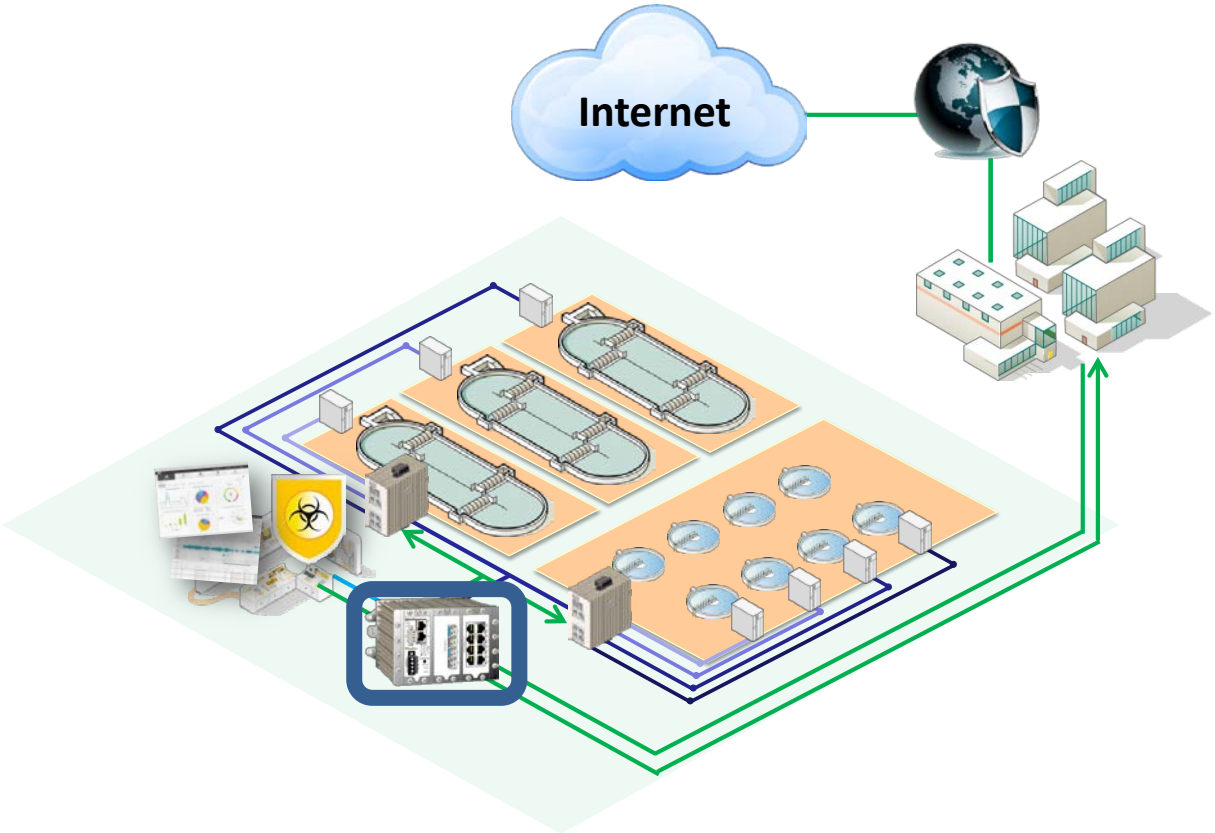

Figure 2 - WeOS Target for Perimeter Protection

In this scenario, no connection requests at all are allowed from the office in to the production network and connection requests from the production network going out is strictly controlled in terms of source, destination, port and protocol. All known bad and unknown connection requests from the production network to the outside should be logged to an intrusion detection system.