ICS Defense Use Case (DUC) Dec 30, 2014

Authors:

Robert M. Lee
Michael J. Assante
Tim Conway

ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper –

German Steel Mill Cyber Attack

Note: We are providing a summary of the available information and are basing the details of the incident on the publicly available report. Open-source data gathered throughout 2014 regarding incidents can reveal information about the potential identity of the facility in question. However, the identity of the facility was not released and in an effort to protect the privacy of those involved none of the other open-source information will be presented in this report. The identity of the facility and specific process are not important to establishing lessons-learned.

Incident Summary

In December, 2014 the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI) (translated as Federal Office for Information Security) released their annual findings report.[1] In one case they noted that a malicious actor had infiltrated a steel facility. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network. According to the report, the adversary showed knowledge in ICS and was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage.

To date, the only other public example of a cyber attack causing physical damage to control systems was Stuxnet. As such, the BSI's reporting of this incident generates a useful case-study to extract lessons learned for the community.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile (See Appendix for Translated Text)

Credibility: 4 - The available information and reporting is being evaluated as probably true. So far the BSI is the only source to have reported the incident and the details of the story cannot be corroborated in other publicly available information. However, the BSI is a government agency and has shown accuracy with regards to incident reporting. Simple credibility rating system.[2]

Amount of Technical Information Available: 2- The information available provides details of how the intrusion took place into the corporate network. However, the report does not discuss the attack methodology in the plant network nor does it release technical details. Simple descriptive rating system[3]

[2] Credibility of the information is rated in a scale from [0] Cannot be determined, [1] Improbable, [2] Doubtful, [3] Possibly true, [4] Probably true, [5] Confirmed

[3] Amount of technical information available is an analyst's evaluation and description of the details available to deconstruct the attack provided with a rating scale from [0] No specifics, [1] high-level summary only, [2] Some details, [3] Many details, [4] Extensive details, [5] Comprehensive details with supporting evidence

Attacker Tactics, Techniques, and Procedures (TTPs) Description

The original German report did not provide details about the attacker nor their TTPs, but we should consider their evaluation of the attacker's knowledge regarding ICS.

Attacker - There is no definitive evidence attributing the attacker to specific individuals or organizations. The BSI described the incident as an "APT[4]-Attack" but no discussion of motive has been publicly released. From the information release if we characterize and evaluate one possible profile for the actor as an APT threat actor with a typical focus on intellectual property theft, not intentional process damage. For this reason, we can possibly consider an adversary that utilizes traditional APT tactics and tools, however their ultimate goal is beyond intellectual property theft.

Capability - The initial capability used to infiltrate the facility's corporate network was a phishing email. The BSI's report described this attack vector as "an advanced social engineering" attack which multiple attackers used to gain access to the network. The adversaries then worked their way into the production (ICS) networks. From previous analysis of spear-phishing related incidents with ICS facilities it is highly likely that the email contained a document such as a PDF that when opened executed malicious code on the computer. This malicious code would have then opened up a network connection for the attacker(s) unbeknownst to the facility's personnel. No information has been presented on how the adversary moved into the production network but analysis of similar case-studies would indicate probable traversal through trusted zones and connections between the corporate and plant network. Details of the target's architecture and services along with attacker techniques would be very valuable to assist in additional defensive learning. Consideration of the steel industry and the massive scale of facilities and operating environments is an important area to evaluate when examining this event. For example, if this was an integrated steel mill with a large number of process environments or if this was a mini-mill environment, or a rolling mill environment, there is a significant difference in the process scale and the corresponding scale of attack vectors (for a basic description of the operational differences see the reference on mini-mills[5]). The translated report makes note of an impacted furnace, however does not provide further detail on the type (blast furnace, basic oxygen furnace, arc furnace) and therefore does not provide enough information to determine the type of damage that could have been caused by mis-operating the process specifically.

[4] Advanced Persistent Threat (APT) is a description that has been used by NIST to describe highly targeted attacks that often have full time staffing and monetary support to pursue operations usually for the purpose of espionage.

[5] http://web2.geo.msu.edu/geogmich/minmills.html

Opportunity - Corporate networks present a highly valued target for adversaries interested in ICS. Corporate networks often have connections into, or important credentials for, the ICS network that adversaries can exploit. Many of these process networks were built as separate islanded systems that allowed necessary communications from higher level process networks as required for operations or control. Over time business requirements for additional visibility, ordering, scheduling, and remote support have required additional communications from traditional IT networks into the process control networks. Adversary groups have demonstrated capability to pivot from these higher-level networks into the operational networks through these trusted communications channels. In the event that networks are not connected, the data that exists on corporate networks is useful to attackers; this information can include ICS specifications or schematics as well as personnel data such as emails and network information that can be used to attempt another attack vector. In this case-study, the adversary exploited target personnel's willingness to open untrusted emails to gain access to the network and then the corporate network's connection to the plant network.

Motivation – No information has been publicly presented on the attacker(s)' motivation. Multiple theories can be drawn including industrial sabotage for competing contracts or national interests, environmental extremists, or an individual or group testing out capabilities and tactics whether the physical damage was intended or not. It is unlikely that the attacker was a disgruntled employee or insider threat given the initial attack vector of a phishing email. An insider threat would have had more accessible and non-attributable means to cause havoc in the network. However, at this point very few theories can be ruled out. The motivation becomes a very interesting dimension if damaging the operation was actually the attacker's goal. While a number of facilities have undoubtedly experienced an event that caused some level of operational impact, that was the result of equipment failure or human error, and most are recovered from quickly. What is interesting in the report is the wording that the attackers had advanced know how in ICS and knowledge of the process and most importantly were able to achieve massive damage to the process. The description in the BSI report and accompanying knowledge on process incidents leads the authors to believe the process damage was intentional.

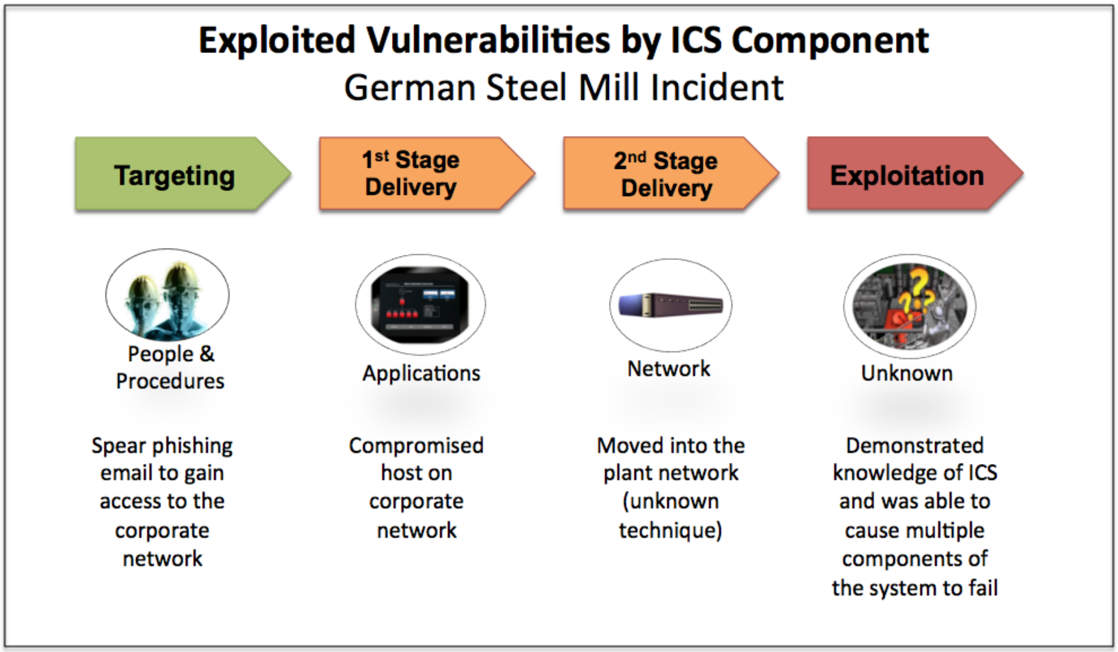
Attack Surfaces & Paths

According to the report the exploitation of the German steel mill took place by targeting on-site personnel in the corporate network. The BSI report also stated that the targeted group were industrial operators. Adversaries targeted the personnel with spear phishing emails. Recent ICS-targeted technical threats have included this style of targeting with phishing emails as was observed in the HAVEX[6] and BlackEnergy2[7] campaigns. Targeting and delivery techniques have focused on specific individuals, trusted relationships with ICS and industrial suppliers, and the need to download files.

The phishing emails would have contained a document that hosted malicious code. Once opened the malicious code would have targeted a vulnerability in an application on the target's system. Once the application was exploited the target system would have opened a remote connection point allowing adversaries access to the network. The second stage of the attack would have involved the adversary accessing the network and, as observed in previous cases, establishing a foothold on the network through the compromise of small sets of workstations. Internal reconnaissance by the adversary from these systems would have provided access of credentials or unsecured systems and connections. This type of reconnaissance is typically performed through the use of keyloggers, network scanning, and the compromising of systems such as Active Directory. The second stage of moving into the plant network and final stage of the attack leading to the physical damage is unknown (see Figure 1).

To help defenders better visualize an adversary performing these attack steps, and pivoting through a business network please reference a free SANS cyber-attack video that was put together for utility control systems, however it is applicable to the steps and approach discussed throughout this defense use case. http://www.securingthehuman.org/cyberattackdemo

[6] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
[7] http://www.critical-intelligence.com/resources/papers/CI-Sandworm-BE2.pdf



Exploited Vulnerabilities by ICS Component

German Steel Mill Incident

Targeting → 1st Stage Delivery → 2nd Stage Delivery → Exploitation

People & Procedures

Spear phishing email to gain access to the corporate network

Applications

Compromised host on corporate network

Network

Moved into the plant network (unknown technique)

Unknown

Demonstrated knowledge of ICS and was able to cause multiple components of the system to fail

Figure 1: Exploited Vulnerabilities by IT/ICS Component

Impacted Systems & Functions

The source stated there was: "an accumulation of breakdowns of individual components of the control system or of entire facilities." The furnace was then unable to be shut down properly which resulted in unexpected conditions and physical damage to the system. See Figure 2 for a description of Steel Mill operations.

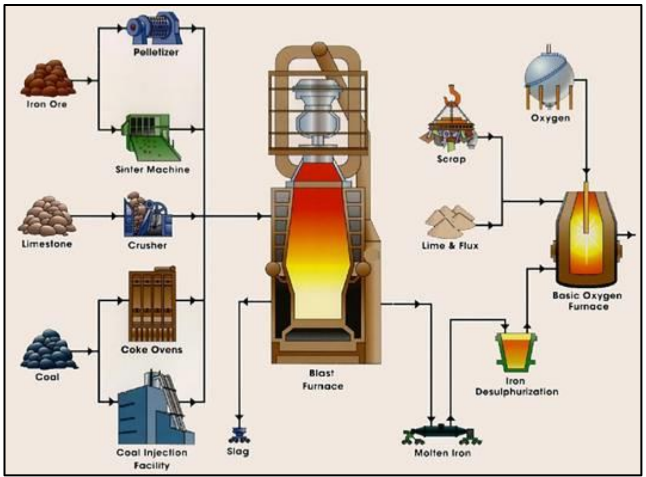


Figure 2: Integrated Steel Mill[8]

[8] http://intranet.bmg.vic.edu.au/wiki/index.php?title=Mill_machining#Steel_Mill

Systems that were known to have been impacted:

- Individual control system components
- Furnace (uncertain on type based on translated report)

Components that were also possibly impacted given the scenario:

- Centralized controls based on a Programmable Logic Controller (PLC)
- Alarm systems
- Safety Instrumented Systems (SIS)
- Human Machine Interface (HMI)
- The individual control system functions could have been one or more:[9]
    - Burden control
    - Burden distribution
    - Mass and energy balances
    - Kinetic process models
    - Hot-blast system

The combined impact may have resulted in a Loss of Control (LoC) for plant operators and possible malicious control leading to physical destruction.

Example Blast Furnace Safety Incident (non-cyber attack related)

Figure 3 and Figure 4 show an example blast furnace to assist in visualizing these systems and their individual components. Both images are taken from a report prepared by the United Kingdom's (UK) Health and Safety Executive office regarding the explosion of blast furnace Number 5 that took place at Corus UK Ltd, Port Talbot, UK on November 8th, 2001.

[9] The list is generated from lists of known steel plant components related to blast furnaces and not from direct reporting on this specific case-study.

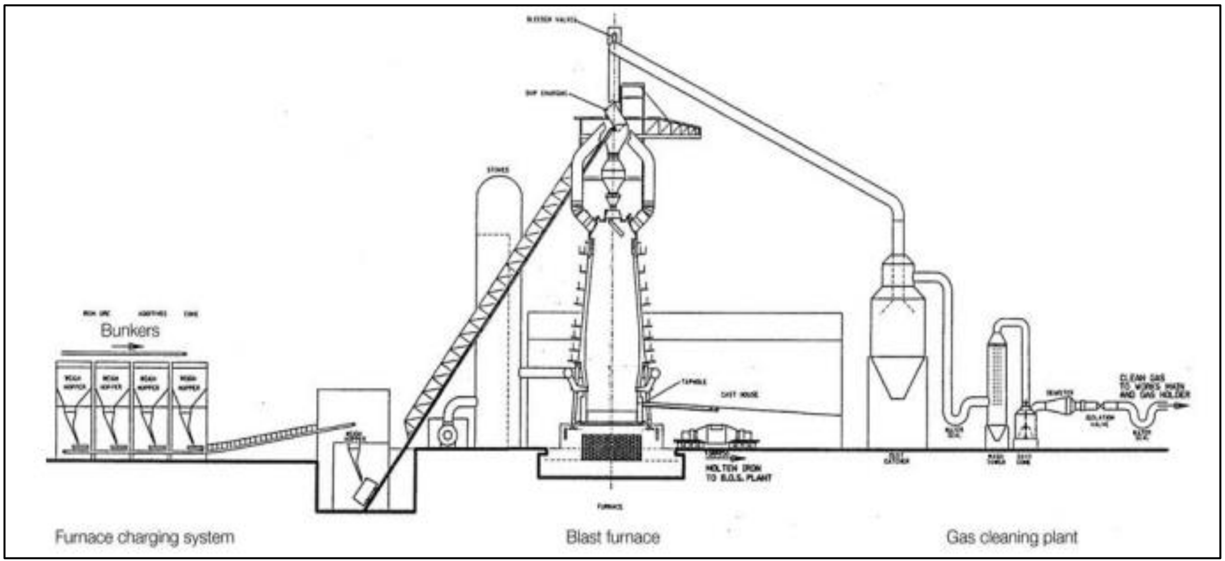


Figure 3: Example "Column-Supported" Blast Furnace[10]

This tragic event claimed the lives of two while injuring thirteen others. This incident was not related to a cyber attack but the UK's report highlights the potential impacts of blast furnace explosions and various lessons learned regarding incident response and safety.

[10] http://www.hse.gov.uk/pubns/web34.pdf

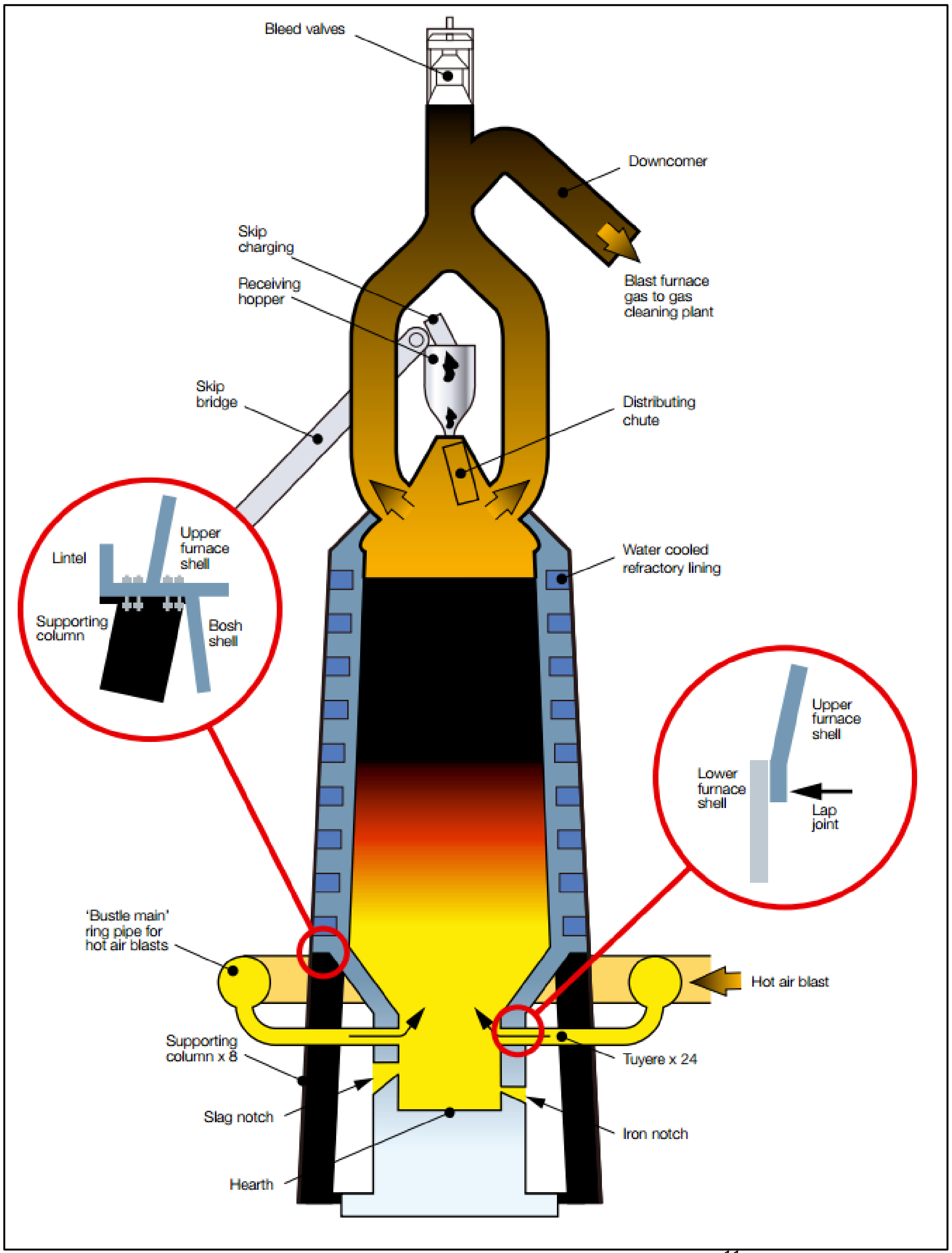


Figure 4: Example Close-Loop Blast Furnace[11]

[11] Ibid.

Defense Lessons Learned

The German steel mill cyber attack is significant because of the physical damage that resulted as well as the German government's willingness to release information regarding the incident. Sharing incident reports is extremely valuable to deriving lessons learned and best-practices for defense and incident response. Even though this example lacks technical details it provides multiple learning points for defender's to consider. Regardless of facility type or sector, the most significant component of this report is the demonstrated capability and willingness of an attacker to attack through traditional APT style methods and then advance to a cyber physical attack with an intent to impact an operational environment.

Technical:

Architecture – The corporate network's connection to the plant network provided the attacker the opportunity to impact the process and physically damage systems. Air gaps have long been discussed in the ICS community but are largely not feasible and are unreliable (at a minimum files often move across these gaps). However, connections that must exist between networks should be heavily regulated through the use of a demilitarized zone (DMZ) with specially tuned firewalls, focused monitoring, and defense systems. Specifically, access points into the network should be documented, controlled, monitored, and limited. The limitation of these access points creates defined points in and out of the network that creates chokepoint type functionality.

Network Security Monitoring – Proper architecture, such as limited access points or chokepoints, creates opportunities for network security analysts to collect and monitor data traversing networks and network data internal to the ICS IP-network. Network Security Monitoring (NSM) allows for analysts to actively view and understand network communications to identify anomalies and adversary tactics. Attackers that traversed from the corporate network to the plant network could have quickly been identified by NSM tactics. Additionally, the attackers' movement inside the plant network, including any scanning to perform network reconnaissance, would have also been identifiable. A very powerful defender's advantage for ICS is to control and monitor all egress traffic from the more trusted network. Another powerful tool is to establish a 'canary' host on the ICS network that has no other purpose then to behave as a tripwire if the machine is accessed or communicated to or from.

Incident Response – In the scenario, the operations personnel on site presumably realized that a cyber-related incident may have occurred as at some point they made contact with the BSI. This likely reflects great professionalism on the part of both the BSI and the facility's members. Additionally, it is worth noting that there was no indication of harm to human life, which indicates responsible and reliable engineering of physical safety systems. The learning point though is that while this infrastructure may have been critical to the organization it was likely not to be considered critical infrastructure. Yet, adversaries targeted it and caused significant damage. Defenders do not get to choose whether or not they make good targets; only attackers get to decide. It is important to have incident response plans ahead of time including the incorporation of cyber-attack scenarios. These plans pay dividends to ensure the reliability and safety of infrastructure while discerning root causes of incidents to better future defense.

People:

Security Awareness/Base Knowledge – All of cybersecurity efforts begin with people and it is where many cyber incidents also begin. The development of an overall cybersecurity strategy to protect both the corporate network and plant systems begins with system owners and cybersecurity specialists. The susceptibility of deployed technology can lie purely in the technology, but in many cases it can be a combination of how the technology is configured or through actions taken by authorized system users and administrators. Many of the recent ICS-focused technical threats have included targeting and delivery techniques that have focused on human and work practice vulnerabilities. Attackers look for easy paths to gain footholds on trusted networks and place themselves within reach of important data and credentials that can help them achieve a freedom of movement and action.

This report states that operators of industrial plants were targeted and highlights the need for both corporate system and plant system users to receive and demonstrate competency in security awareness and base cybersecurity knowledge as it applies to their individual role. There are strong arguments for providing this training based on the type of work being performed and using the language that best aligns to the context of the technology and operation. Developing engineering focused modules allows security program managers to relate common day-today activities to secure and less secure behaviors.[i] It is important to address issues like remote access procedures, downloading technical data sheets or software/firmware from the Internet, providing publicly available information, etc.

Implications / Predictions

The incident reported by BSI has profound implications for ICS defenders as the incident points to cyber actors that are knowledgeable of targeting and delivering cyber attacks against ICS as well as possibly effecting controlled equipment. The use of highly successful APT TTPs to move from the corporate network into the plant network validates a primary attack vector into ICS. Attackers will continue to use trusted connections and harvest information and credentials to compromise more trusted networks. Several North American cyber incidents have also pointed to ICS capable and interested attackers compromising corporate networks via spear phishing and waterhole styled attack vectors.

More ICS-capable attackers will be coming to light in the coming years as the community becomes more open with sharing incidents. Only a few will seek to physically damage equipment under control but each pose serious threats to impacting the process either intentionally or accidentally.

Conclusion

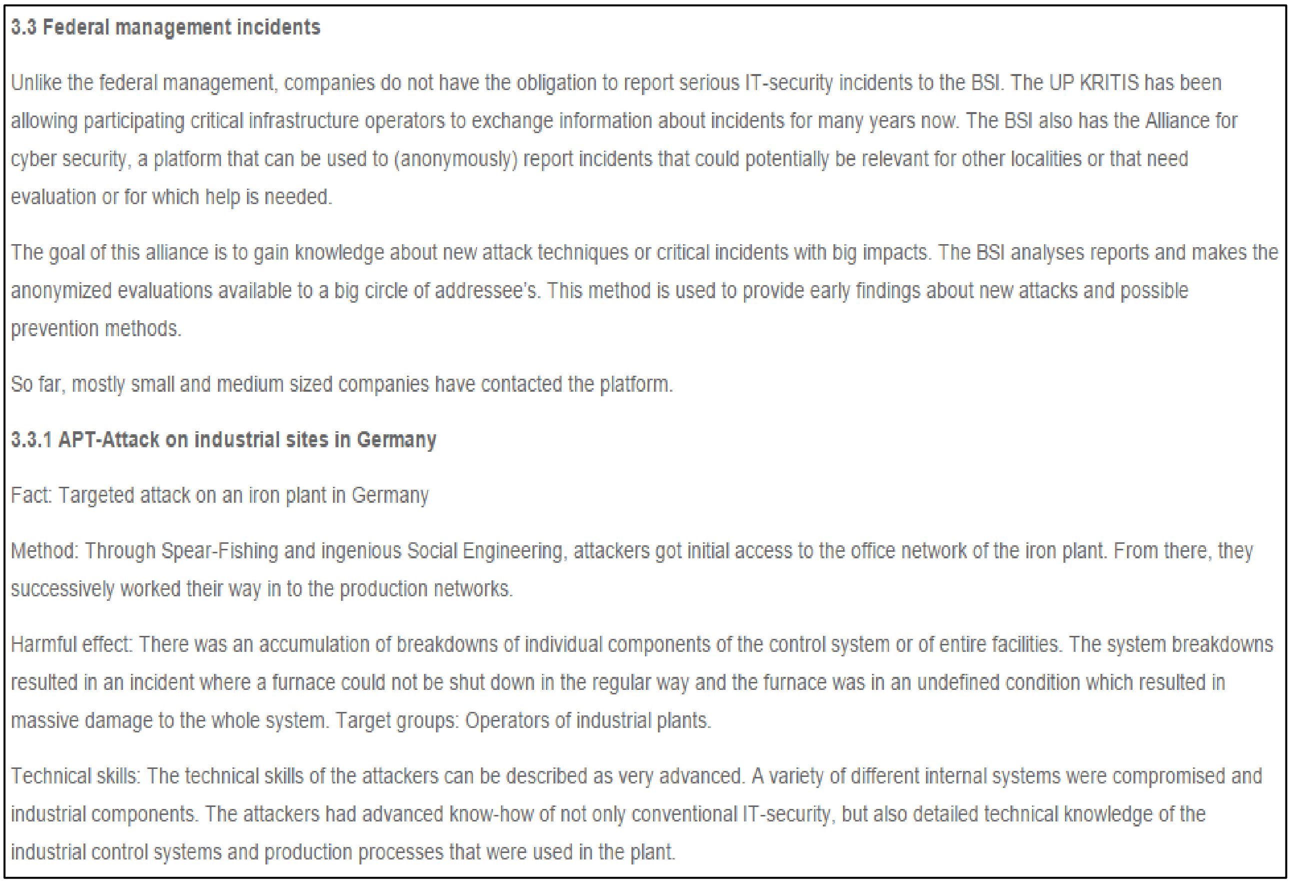
The authors thank the BSI for publishing information about this incident and requests consideration to release more detailed information to assist in developing lessons learned. Likewise, organizations across the various ICS industries are asked to find an appropriate way to share incident case-studies and best practices developed. In many industries this can be done safely through the industry specific Information Sharing and Analysis Centers (ISACs). If an appropriate way forward is not identifiable please feel free to contact the authors of this report without including specific or sensitive information; the authors will make points of contact available for assistance.

More information will help focus recommendations and lessons that can be relayed to asset owners and operators. ICS-capable and targeted cyber attacks represent a threat that exceeds existing ICS security best practices. Many security controls are static in nature and are much more effective in combating less structured, non-targeted, cyber attacks. ICS defenders will need to enhance their security capabilities moving beyond the perimeter defense model and addressing how people interact with and expose ICS to cyber threats.

Follow us on Twitter for additional updates:
https://twitter.com/SANSICS
https://twitter.com/robertmlee

SANS
10TH ANNUAL
ICS SECURITY
SUMMIT & TRAINING
Orlando, FL | SUMMIT: Feb 23-24 | TRAINING: Feb 25 - Mar 2
For SCADA, Industrial Automation, and Control System Security

Appendix: Translated Text from BSI Report



3.3 Federal management incidents

Unlike the federal management, companies do not have the obligation to report serious IT-security incidents to the BSI. The UP KRITIS has been allowing participating critical infrastructure operators to exchange information about incidents for many years now. The BSI also has the Alliance for cyber security, a platform that can be used to (anonymously) report incidents that could potentially be relevant for other localities or that need evaluation or for which help is needed.

The goal of this alliance is to gain knowledge about new attack techniques or critical incidents with big impacts. The BSI analyses reports and makes the anonymized evaluations available to a big circle of addressee's. This method is used to provide early findings about new attacks and possible prevention methods.

So far, mostly small and medium sized companies have contacted the platform.

3.3.1 APT-Attack on industrial sites in Germany

Fact: Targeted attack on an iron plant in Germany

Method: Through Spear-Fishing and ingenious Social Engineering, attackers got initial access to the office network of the iron plant. From there, they successively worked their way in to the production networks.

Harmful effect: There was an accumulation of breakdowns of individual components of the control system or of entire facilities. The system breakdowns resulted in an incident where a furnace could not be shut down in the regular way and the furnace was in an undefined condition which resulted in massive damage to the whole system. Target groups: Operators of industrial plants.

Technical skills: The technical skills of the attackers can be described as very advanced. A variety of different internal systems were compromised and industrial components. The attackers had advanced know-how of not only conventional IT-security, but also detailed technical knowledge of the industrial control systems and production processes that were used in the plant.

[i] SANS has developed specific training for both cyber security professionals and plant technical staff along with focused Secure The Human (STH) modules for Engineers. Additionally, SANS has introduced ICS410: ICS Security Essentials and the Global Industrial Cybersecurity Professional (GICSP) to provide and test essential ICS cybersecurity knowledge for IT personnel, OT support, and engineering staff.