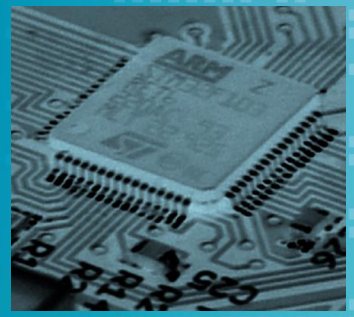





22. VDE Symposium Netzleittechnik / Symposium Informationstechnik 2023
15.06.2023

IT-Sicherheitsbewertung einer digitalen Station: Methodik und Erfahrungen

Adam Bartusiak M.Sc.
Fraunhofer IOSB-AST, Abteilung Kognitive Energiesysteme

Agenda

1. Hintergründe und Motivation
2. Vorgehensweise
3. Ergebnisse
4. Zusammenfassung

IT-Sicherheitsbewertung einer digitalen Station

Hintergründe und Motivation

Projektdetails

- *Auftraggeber: Thüringer Energienetze (TEN)*
  - *Verpflichtet als KRITIS-Versorgungsnetzbetreiber nach EnWG §11 Ab. 1a*
    → *„…einen angemessenen Schutz gegen Bedrohungen für IKT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, zu etablieren“*
- *Aufgabe:*
  - *Detaillierte* **Untersuchung der Sicherheitsaspekte** *konkreter Fernwirktechnikelemente*
  - *Betrachtung aktueller Normen der IT-Security (ISO/IEC 27002, 27019 und IEC 62443, BDEW Whitepaper)*

- *Ziele:*
  - **Überprüfung der Assets auf Schwachstellen** *und mögliche Sicherheitsdefizite*
  - *Erarbeitung eines* **Netzwerk-Security-Konzepts** *für die Fernwirktechnik*
  - **Entwicklung einer standardisierten Methodik** *für Sicherheitsanalysen von anderen IKT-Systeme*

IT-Sicherheitsbewertung einer digitalen Station

Hintergründe und Motivation

Konventionelle GAP-Analyse (Compliance-Check)

- **Auswahl** *eines geeigneten* **Sicherheits-Frameworks** *als Hauptbezugspunkt*
- *Priorisierung und Auswahl relevanter* **Sicherheitsanforderungen**
- **Prüfung des aktuellen Umsetzungsstandes** *und* **Ermittlung der Unterschiede** *(Lücken) zu den entsprechenden externen Anforderungen aus einem ausgewählten Sicherheitsstandard*

→ IT-Sicherheitsbewertung einer digitalen Station:

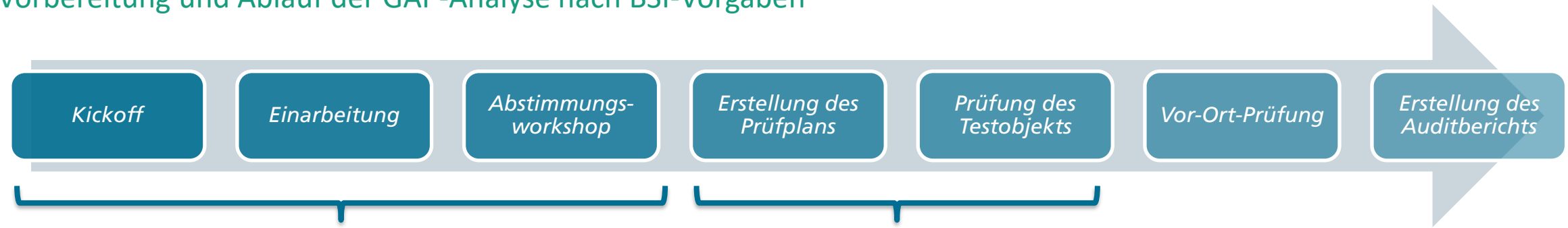
Erweiterung der GAP-Analyse zu einer technischen Sicherheitsanalyse mit Einbeziehung verschiedener Sicherheitsnormen und -vorgaben

- *allgemeine Normen: IT-Grundschutz, ISO/IEC 27002, IEC 62443, NIST SP 800-115, NIST SP 800-53*
- *spezifische Normen: ISO/IEC 27019, IEC 62351, BDEW-Whitepaper, NESCOR-Fachbericht*
- *Forschungspublikationen*
- *Technische Richtlinien*

IT-Sicherheitsbewertung einer digitalen Station

Vorgehensweise

Vorbereitung und Ablauf der GAP-Analyse nach BSI-Vorgaben*



- → **Scope der Überprüfung**
- → *Rules of Engagement*
- → *Überprüfung der Dokumentation*
- → *Vorschlag zum Prüfungsablauf*

- → **Erstellung eines detaillierten Testplans**
- → *Festlegung eines standarisierten Formats für die* **Beschreibung und Dokumentation von Testfällen**

  - Referenzdokumente, -Dateien, -Software, -Hardware
  - Ausgangsbedingungen / Parametrierung
  - Beschreibung der einzelnen Testschritte
  - Testergebnisse

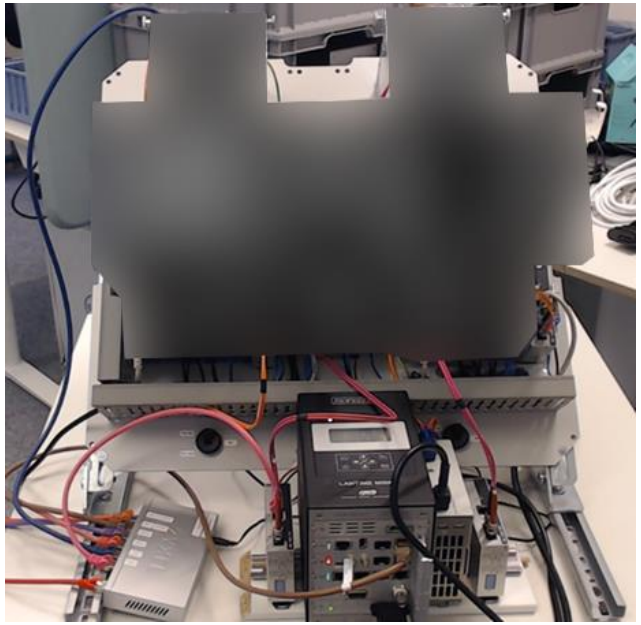
**ICS-Security-Kompendium, Bundesamt für Sicherheit in der Informationstechnik - Methodik für Audits von ICS-Installationen*

Fraunhofer IOSB

IT-Sicherheitsbewertung einer digitalen Station

Scope der Überprüfung

- *Sicherheitsanalyse eines redundanten Systems zur Datenkopplung zwischen Unterstationen, Umspannwerken und Netzleitstellen…*
  - *…an einem* **Testaufbau** *als Nachbildung der Originalanlage*
    → *Gerätesicherheitsanalyse*
    → *Netzwerksicherheitsanalyse*
  - *…bei einer* **Vor-Ort-Besichtigung**
    → *Analyse der physischen Sicherheit*



IT-Sicherheitsbewertung einer digitalen Station

Erstellung des Testplans: Bewertungstechniken

Informations-auswertung

- *Verifizierung von Maßnahmen zur sicheren Konfiguration und Härtung*
- *Detaillierte Übersicht über die installierten Systeme und Anwendungen*

Passive Prüfmethoden

- *Sicherheitsreview von Dokumentation, Logdateien, Regeln, Systemparametrierung*

Schwachstellen-analyse

- *Überprüfung des Ist-Stands von den dokumentierten Komponenten/Diensten*
- *aktive, manuelle oder automatische Identifizierung möglicher Schwachstellen*

Aktive Prüfmethoden

- *Ermittlung von Ports und Diensten*
- *Analyse des Netzwerkverkehrs*
- *Verwendung von Schwachstellen-Scannern*

Aktive Eindring-versuche

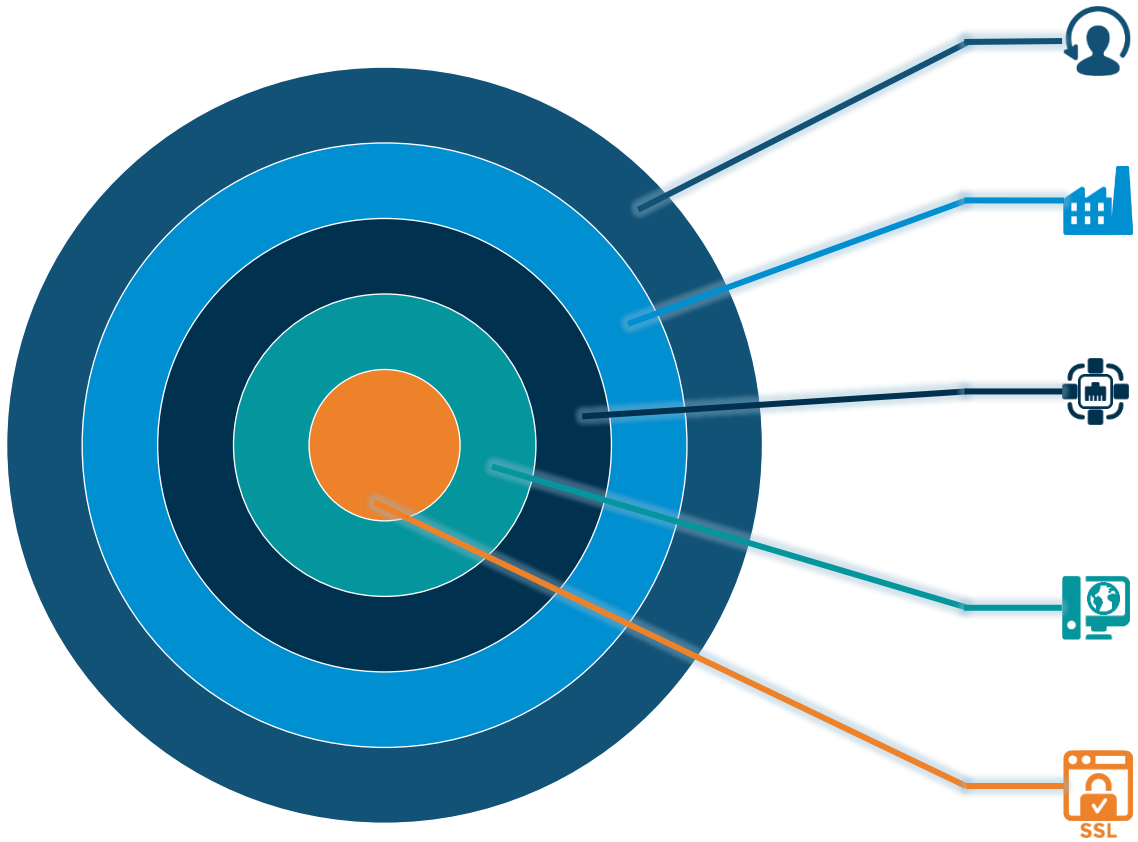
- *Verifizierung der potenziellen Schwachstellen hinsichtlich der Risiken*
- *Anwendung bestehender und selbst entwickelter Angriffe auf ausgewählte Systeme und Protokolle*

Gezielte Angriffe

- *Denial-of-Service-Angriffe*
- *Man-in-the-Middle-Angriffe*
- *Fuzzing-Angriffe*
- *Kompromittierung von Zugangsdaten*

IT-Sicherheitsbewertung einer digitalen Station

Erstellung des Testplans: Sicherheitsebenen nach Defense-in-Depth



Faktor Mensch: Policies, Prozesse und Security Awareness
- *Risikomanagement, Incident Response Management*
- *Standards und Empfehlungen*
- *Schulungen*

Physische Sicherheit
- *Zugangskontrollen*
- *Zäune, Schließsysteme, Alarmanlagen*
- *Videoüberwachung*

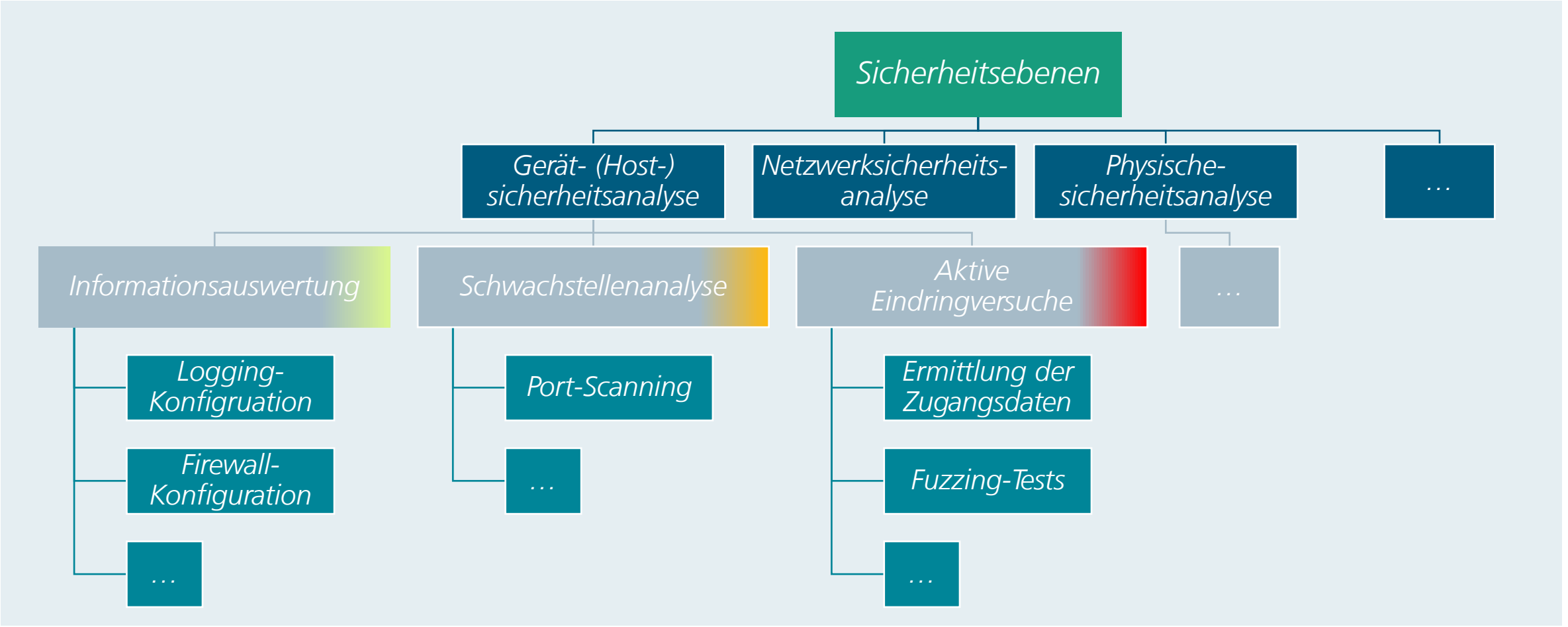
Netzwerk-Sicherheit (Unternehmen + ICS)
- *"CyberSecurity Architektur"*
- *Firewall, VLAN, DMZ*
- *VPN, IDS/IPS*
- *Monitoring, SIEM*

Host-Sicherheit
- *Patch-Management*
- *Antivirus, Whitelisting*
- *Server, Arbeitsplatz, Feldgeräte, VMs*

Anwendungs- und Datensicherheit
- *Identitätsmanagement*
- *Zugriffskontrolle*
- *Verschlüsselung*

IT-Sicherheitsbewertung einer digitalen Station

Erstellung des Testplans: Sicherheitsebenen nach Defense-in-Depth



Fraunhofer IOSB

IT-Sicherheitsbewertung einer digitalen Station

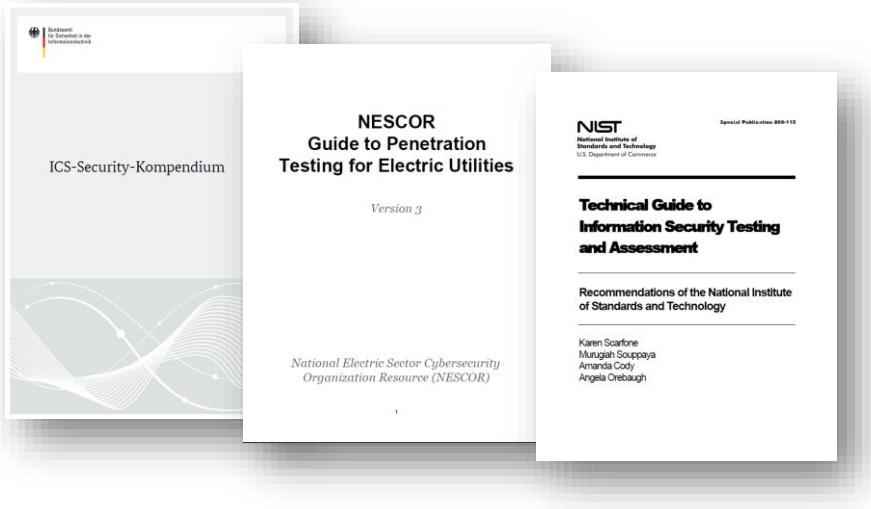
Erstellung des Testplans: Beispiel Darstellung

ID	Prüfungspaket (PP)	Ziele	Prüfungsschritt	ID	Prüfungsaspekt (PA)	Prüfungsdetails	Prüfwerkzeuge	Risiken
PP0	**Vorbereitungsarbeiten**							
PP1	**Informationsbeschaffung und -auswertung**	* Verifizierung von Maßnahmen zur sicheren Konfiguration und Härtung * Detaillierte Übersicht über die installierten Systeme und Anwendungen/Dienste inklusive der potenziellen Angriffspunkte bzw. der bekannten Sicherheitsmängel * Ermittlung möglicher Schwachstellen	Parametrierung und Konfiguration	PA1	Firmware & Patchversion	* Abgleich mit der Dokumentation * Abgleich mit der Sprecher-Schwachstellenliste und CVE-Datenbank (https://www.sprecher-automation.com/de/it-sicherheit/)	Manuelle Prüfung	Keine
				PA2	Netzwerk-Einstellungen	* Abgleich mit der Dokumentation		
				PA3	Firewall-Einstellungen	* Abgleich mit der Dokumentation * Analyse der FW-Regeln		
				PA4	Logging-Einstellungen	* Logqualität * Sicherheitsrelevante Ereignisse		
				PA5	Benutzerzugänge	* Passwortqualität (Verwendung von Standard-Passwörter) * Überprüfung der Passwortdateien		
				PA6	Nutzerrollen	* Korrekte Zuordnung von Privilegien zu Rollen (Freigabe- und Verzeichnisberechtigungen)		
			Netzwerkschnittstellen	PA10	Netzwerkverkehr in einzelnen Schnittstellen	Aufzeichnung von Daten (Packet Sniffing): * Endpunkte korrekt verzeichnet? * Datenvolumen korrekt? * Legitime Datenverbindungen? * Replay, MinM-Angriffe möglich? * Welche Daten werden unverschlüsselt übertragen? * Zielgeräte: ZLG	Sniffing: * SPAN Port * Hak5 Plunder Bug * Wireshark	
				PA11	Ermittlung von Ports und Diensten	Port-Scanning: * Alle Dienste verfügbar? * Nicht dokumentierte Dienste vorhanden? * Zielgeräte: ZLG	Netzwerkscanner: * Nmap	* Funktionsstörung * Unerwartete Ereignisse * Verfügbarkeits-einschränkungen
PP2	**Schwachstellenanalyse**	* Verifizierung von Maßnahmen zur sicheren Konfiguration * Überprüfung des Ist-Stands von den dokumentierten Komponenten/Diensten * Ermittlung möglicher Schwachstellen		PA12	Webbasierte Schwachstellen	OWASP Schwachstellen: * XSS, SQL-Injection * Pufferüberlaufe * Inputvalidierung * Zielgeräte: ZLG	Web-Schwachstellenscanner: * Nikto * Burp Suite * OWASP ZAP	
				PA13	Ermittlung ausnutzbarer Schwachstellen	* Veraltete Versionen von Anwendungen/Dienste? * Bekannte Schwachstellen? * Zielgeräte: ZLG	Schwachstellenscanner: * OpenVAS * Nessus	
PP3	**Aktive Eindringversuche**	* Aktiver Angriff auf ausgewählte Systeme * Verifizierung der potenziellen Schwachstellen hinsichtlich der tatsächlichen Risiken	Geräteverfügbarkeit	PA14	Denial of Service	* TCP-SYN-Flood * Ping of Death * Zielgeräte: ZLG	Packet crafting: * Hping * Scapy	* Funktionsstörung * Unerwartete Ereignisse * Verfügbarkeits-einschränkungen
			Kompromittierung von Zugangsdaten	PA15	Zugang erlangen	* Passwort-Bruteforce * Validierung Reset-Optionen * Plain- und Hashwerte abgreifen (MinM-Angriff) * Zielgeräte: ZLG	* John the Ripper * Ettercup * Scapy * Custom Skripting	
			Netzwerkverkehr-Vertraulichkeit	PA16	VLAN Angriff	* VLAN Hopping * Zielgeräte: ZLG	* Yersinia * Gitlab Projekte	

IT-Sicherheitsbewertung einer digitalen Station

Erstellung des Prüfplans: Referenzdokumente

- *Referenzdokumente zur Prüfplanerstellung*
  - *BSI - ICS-Security-Kompendium*
  - *BSI – A Penetration Testing Model*
  - *NIST – Technical Guide to Information Security Testing and Assessment*
  - *NESCOR - Guide to Pentration Testing for Electric Utilities*
  - *Hahn A., Govindarasu M. – Vulnerability assessment for substation automation systems*



- *Forschungspublikationen zur inhaltlichen Gestaltung der Tests*
  - *Testing and Exploring Vulnerabilities of the Applications Implementing* **IEC 60870-5-104** *Protocol - Bin, Zi.*
  - *Towards Understanding Man-In-The-Middle Attacks on* **IEC 60870-5-104** *SCADA Networks - Maynard, P. & Mclaughlin, K, Et al.*
  - *Attacking* **IEC-60870-5-104** *SCADA Systems - Radoglou G., Panagiotis & Sarigiannidis, Panagiotis & Giannoulakis, Et al.*
  - *Attacking the* **Network Time Protocol** *- Malhotra, A.*
  - *The Security of* **NTP's Datagram Protocol** *- Malhotra, A. & Gundy, M. & Varia, M. & Kennedy, H. & Gardner, J. & Goldberg, S.*
  - *Smarter* **Grid Fuzzing***: Effective Greybox Fuzzing for Power Grid Communication Protocols - Helmke, R.*

IT-Sicherheitsbewertung einer digitalen Station

Beschreibung der Testfälle

Testfallbeschreibung

Testfall-ID	Version	Titel	Testziele	Referenzstandards
TF1	1.0	Muster Testfall	Verifizierung von...	ISO 27002 Musterabschnitte
			Überprüfung der Anfälligkeit...	BSI Grundschutz Musterbausteine SYS.1.1, IND.2.1,...
			Überprüfung der Dokumentation ...	BDEW Musterabschnitte 4.1.2, 4.1.3, 4.1.8

Verfasser	Max Mustermann	
Zielsystem	FWA	
Systemkennung	ZLG -AXYZ XYZ	
Systemkonfiguration	editor: 1.XX SPX (YYYY) / config: X.YZ,2021-03-05...	
Referenzhardware	HW.1	FWA
	HW.2	Windows 10 Pro 10.0.XXXXX
	HW.3	Kali GNU/Linux 2020.X
	HW.4	Meinberg M500 Zeitserver
Referenzdokumentation	RD.1	Muster-Systembeschreibung.docx
	RD.2	Muster-Firewall-Dokumentation.pdf
	RD.3	Muster-Forschungspaper.pdf
	RD.4	https://muster-url/it-sicherheit/
Referenzsoftware	SW.1	WinPP v. 4.0.X.Y
	SW.2	Wireshark v.2.X.Y
	SW.3	Network Time Protocol Daemon für Windows (ntpd.exe)
	SW.4	NTP Time Server Monitor by Meinberg 1.XX
	SW.5	FWA-Webserver
Referenzdateien	RF.1	konfig.ini
	RF.2	ntp.conf
	RF.3	Muster-Screenshot.png
	RF.4	Muster-Dokument.pdf
Ausgangsbedingungen		
Hardware	HW.1 <--> HW.2 Netzwerkverbindung über X7 für Erzeugung des 104- und NTP-Verkehrs über SW.1 und SW.4	
	HW.1 <--> HW.3 Netzwerkverbindung über X7 für Angriffsdurchführung	
	HW.1 <--> HW.4 Netzwerkverbindung über X7	
Software/Programm	Ausführung SW.1, SW.2	
	Konfiguration (s. RF.5) und Ausführung SW.4 in HW.1 als NTP-Server 1, ggf. Überwachung des Dienstes mit SW.4	
	Konfiguration HW.4 als NTP-Server 2	
	Konfiguration SW.1 wie in RF.1 bzw RF.3 (für B.1.2)	
Skripte/Einstellparameter	SPT.1	iec104_mitm_python_musterskript_1.py
	SPT.2	iec104_mitm_python_musterskript_2.py
	SPT.3	iec104_mitm_python_musterskript_3.py
	SPT.4	iec104_mitm_python_musterskript_4.py
Weitere Bedingungen	B.1	Erzeugung des Netzwerkverkehrs in der einzelnen Kommunikationsstrecken
	B.1.1	X7 - Einrichtung HW.2 mit SW.1 als Muster-Kommunikationsstrecke 1
	B.1.2	X7 - Einrichtung HW.2 mit SW.1 als Muster-Kommunikationsstrecke 2
	B.1.3	X7 - Einrichtung NTP-Server 1 mit HW.2 und SW.4 und NTP-Server 2 mit HW.4
	B.2	X7 - Vorbereitung Muster-Angriffe
	B.2.1	Muster-Bedienung: Aktivierung von XYZ zur Übernahme des Netzwerkverkehrs zwischen X und Y
	B.2.1.1	Muster-Patch im Ordner xyz/zyx anwenden
Screencast/Screenshots	SS.1	Muster-Screenshot_2.png

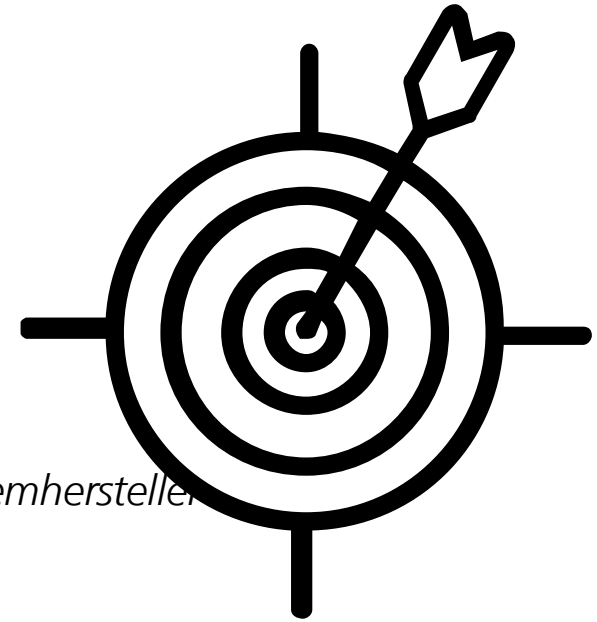
IT-Sicherheitsbewertung einer digitalen Station

Beschreibung der Testfälle

Testablauf														
Schritt	Beschreibung	Schnittstelle / Details	Wert (System)		Wert (Doku)		Ergebni	Anmerkungen	Kritikalit	Weitere Schritte	BC	TF	Anhänge	Screencast/Screens
TS.1	Überprüfung Muster-Dokumentation	Allgemeine Informationen	---	---	RD.3 2.2.1	* Zusammenfassung wichtiger Informationen, die für den Testfall relevant sind * Konfigurationvorgaben/Empfehlungen vom Hersteller * IST/SOLL-Vergleich zwischen Testobjekt und Dokumentation	?	Anmekrungen zum Ergebniss						
TS.2	Vergleich XYZ Muster-Version		SW.5 --> System --> System Information --> Allgemein	0x.ZYXd	RD. 11	0x.ZYXd	OK	XYZ Version-Übereinstimmung						
TS.3	Überprüfung XYZ-Muster-Angriffe	MinM Angriff 1 Skript: SPT.1	Muster-Details Angriff 1	Zusatzinformationen z.B: Angriffsrichtung (IP-Adressen)	RF.4 7 Seite 37 RF.4 V B Seite 6	Beschreibung der Muster-Angriffe in der Dokumentation	TBC	TBC = TO BE CHECKED im anderen TF	Hoch	* Weitere Analyse im relevanten Testfall	TF99		Netzwerk-Mitschnitt Log-Datei	Screenshots-Datei Screencast-Datei
		MinM Angriff 2 Skript: SPT.2	Muster-Details Angriff 2	Zusatzinformationen z.B: Angriffsrichtung (IP-Adressen)			1	Anmekrungen zum Ergebniss	Mittel					
		MinM Angriff 3 Skript: SPT.3	Muster-Details Angriff 3	Zusatzinformationen z.B: Angriffsrichtung (IP-Adressen)			1	Anmekrungen zum Ergebniss	Niedrig					
		MinM Angriff 4 Skript: SPT.4	Muster-Details Angriff 4	Zusatzinformationen z.B: Angriffsrichtung (IP-Adressen)			TBC	TBC = TO BE CHECKED im anderen TF	Mittel	* Weitere Analyse im relevanten Testfall	TF99			
TS.4	Überprüfung TBCs	TF XY Schritt Z - Überprüfung MinM-Angriffe	Keine Sicherheitsmechanismen vorhanden	---	---	---	?	*** Wie in TS.3 geprüft: MinM Angriffe XYZ möglich**						

IT-Sicherheitsbewertung einer digitalen Station

Ergebnisse



Allgemeine Auswertung und Sicherheitsdefizite

- **zahlreiche Integration von Sicherheitsmaßnahmen** *auf mehreren Systemebenen durch Systemhersteller*
- *Umfangreiche Dokumentation von Hersteller zur sicheren Konfiguration der Komponenten*
  - *Best-Practices zu Härtungsmaßnahmen*
  - *Handbuch Informationssicherheit*

- *Sicherheitsdefizite durch* **Anpassung der Konfiguration** *behebbar bzw. vom* **Hersteller unabhängig**, *z. B.:*
  - *inkonsistente Systemdokumentation mit veralteter Konfigurationsinformationen*
  - *unsichere Gerätekonfiguration*
    - *fehlende Regeln in Firewall-Konfiguration*
    - *Protokollierungsrichtlinie, VLAN-Einrichtung, veraltete TLS-Cipher*
    - *unzureichender Schutz der Kommunikationsprotokolle zwischen der Leitstelle und den Fernwirkgeräten (trotz Unterstützung der Verschlüsselungs- und Authentifizierungsmöglichkeiten durch den Hersteller)*

IT-Sicherheitsbewertung einer digitalen Station

Zusammenfassung

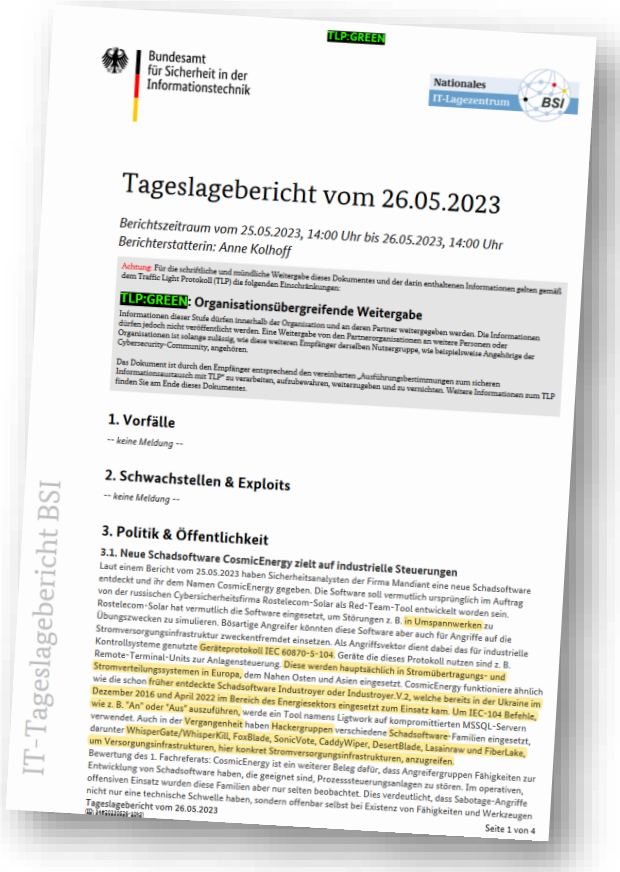
Ergebnisse der Sicherheitsbewertung als Grundlage für:

- **Sichere Konfiguration** *der untersuchten Systeme*
- **Richtlinien zur sicheren Härtung** *der Automatisierungstechnik innerhalb der Organisation*
- *Wissenstransfer und Security-Awareness*
  - *aktuell: Vorbereitung eines* **praktischen Trainings zur Sensibilisierung** *der Mitarbeiter mit TEN-spezifischer Technik als Schulungsdemonstrator*
- *Forschungsmaßnahmen*
  - **Security-Assessment-Framework** *für (teil-)automatisierte Durchführung von Sicherheitsbewertungen im OT-Bereich*

IT-Sicherheitsbewertung einer digitalen Station

Testfall: IEC-104 M-in-M-Angriff

- *Ziel: Überprüfung der Angriffsmöglichkeiten auf das IEC-104-Protokoll*
- **Aktuell: Warnung von BSI im Tageslagebericht**
- *Testumfang*
  - *>10 Varianten von On- und Off-Path-Angriffe*
    - *U-Frame: Reply-Angriffe, DoS-Angriffe*
    - *I-Frame: Manipulationsangriffe, Reply-Angriffe, DoS-Angriffe*
  - *Entwicklung von eigenen Angriffsskripten in Python*


TLP:GREEN

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

Tageslagebericht vom 26.05.2023

Berichtszeitraum vom 25.05.2023, 14:00 Uhr bis 26.05.2023, 14:00 Uhr
Berichterstatterin: Anne Kolhoff

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:GREEN: Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisation und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe, wie beispielsweise Angehörige der Cybersecurity-Community, angehören.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP" zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

1. Vorfälle

-- keine Meldung --

2. Schwachstellen & Exploits

-- keine Meldung --

3. Politik & Öffentlichkeit

3.1. Neue Schadsoftware CosmicEnergy zielt auf industrielle Steuerungen

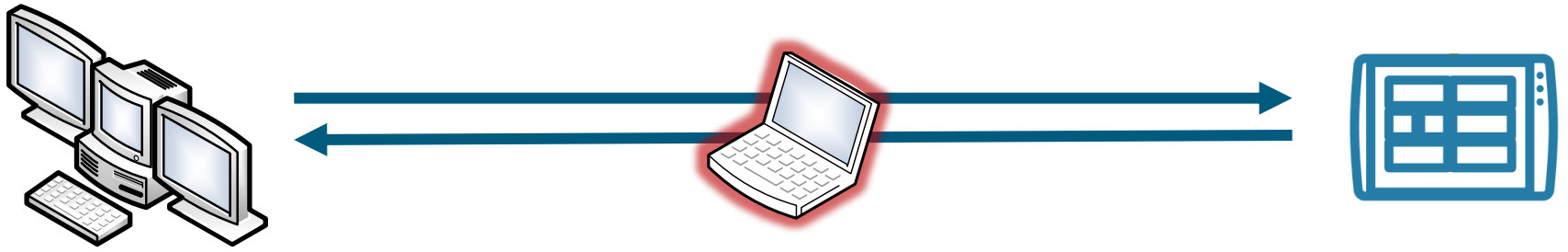
Laut einem Bericht vom 25.05.2023 haben Sicherheitsanalysten der Firma Mandiant eine neue Schadsoftware entdeckt und ihr dem Namen CosmicEnergy gegeben. Die Software soll vermutlich ursprünglich im Auftrag von der russischen Cybersicherheitsfirma Rostelecom-Solar als Red-Team-Tool entwickelt worden sein. Rostelecom-Solar hat vermutlich die Software eingesetzt, um Störungen z. B. in Umspannwerken zu Übungszwecken zu simulieren. Bösartige Angreifer könnten diese Software aber auch für Angriffe auf die Stromversorgungsinfrastruktur zweckentfremdet einsetzen. Als Angriffsvektor dient dabei das für industrielle Kontrollsysteme genutzte Geräteprotokoll IEC 60870-5-104. Geräte die dieses Protokoll nutzen sind z. B. Remote-Terminal-Units zur Anlagensteuerung. Diese werden hauptsächlich in Stromübertragungs- und Stromverteilungssystemen in Europa, dem Nahen Osten und Asien eingesetzt. CosmicEnergy funktioniere ähnlich wie die schon früher entdeckte Schadsoftware Industroyer oder Industroyer V.2, welche bereits in der Ukraine im Dezember 2016 und April 2022 im Bereich des Energiesektors eingesetzt zum Einsatz kam. Um IEC-104 Befehle, wie z. B. "An" oder "Aus" auszuführen, werde ein Tool namens Ligtwork auf kompromittierten MSSQL-Servern verwendet. Auch in der Vergangenheit haben Hackergruppen verschiedene Schadsoftware-Familien eingesetzt, darunter WhisperGate/WhisperKill, FoxBlade, SonicVote, CaddyWiper, DesertBlade, Lasainraw und FiberLake, um Versorgungsinfrastrukturen, hier konkret Stromversorgungsinfrastrukturen, anzugreifen.

Bewertung des 1. Fachreferats: CosmicEnergy ist ein weiterer Beleg dafür, dass Angreifergruppen Fähigkeiten zur Entwicklung von Schadsoftware haben, die geeignet sind, Prozesssteuerungsanlagen zu stören. Im operativen, offensiven Einsatz wurden diese Familien aber nur selten beobachtet. Dies verdeutlicht, dass Sabotage-Angriffe nicht nur eine technische Schwelle haben, sondern offenbar selbst bei Existenz von Fähigkeiten und Werkzeugen

Tageslagebericht vom 26.05.2023

Seite 1 von 4

IT-Tageslagebericht BSI



Fraunhofer IOSB

Kontakt

Adam Bartusiak, M.Sc.
Abteilung Kognitive Energiesysteme
Tel.: +49 3581 374 3586
adam.bartusiak@iosb-ast.fraunhofer.de

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Fraunhofer IOSB-AST, Außenstelle Görlitz
Wilhelmsplatz 11
02826 Görlitz
www.iosb-ast.fraunhofer.de