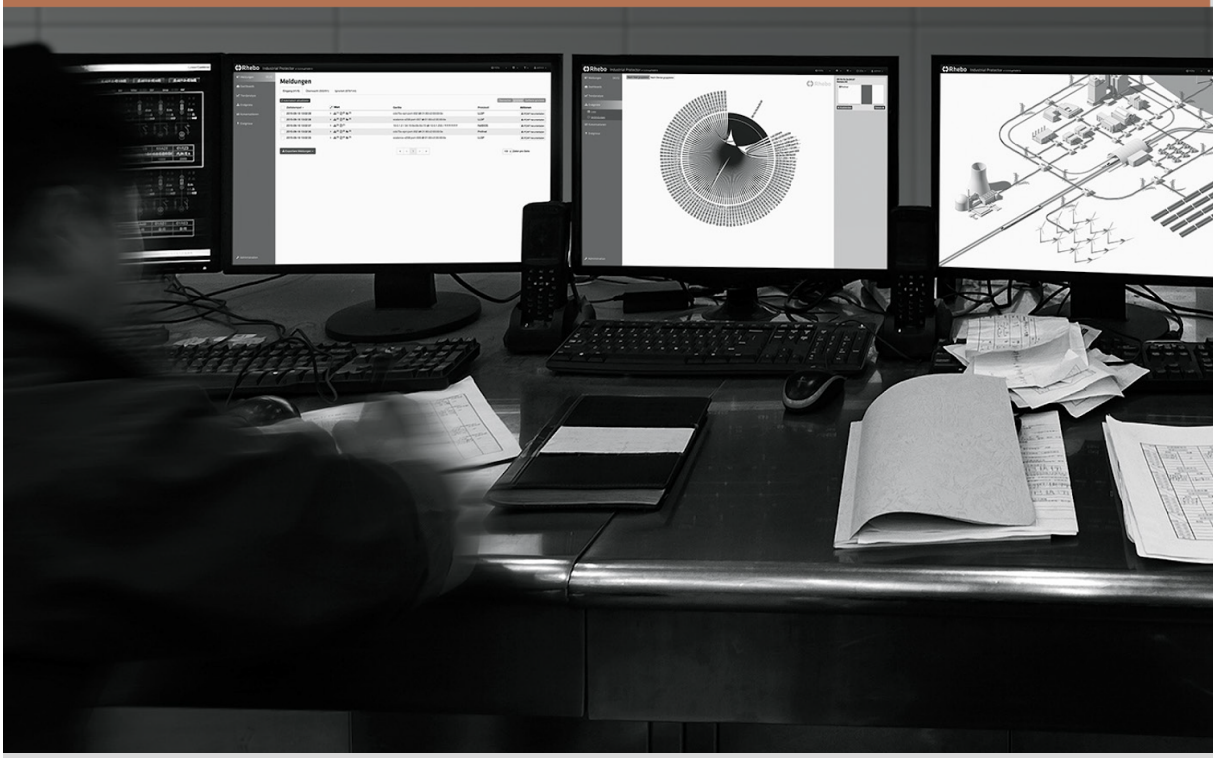
Rhebo Industrie 4.0
Stabilitäts- und Sicherheitsaudit (RISSA)

Ergebnisse und Bewertung

Zur Verfügung gestellt von RHEBO für KUNDE GmbH

RISSA-Analyse des Steuernetzwerks mittels Rhebo Industrial Protector



Inhaltsverzeichnis

Zusammenfassung

Der Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit (RISSA) wurde mittels des bei der KUNDE GmbH am Standort Beispielhausen installierten Rhebo Industrial Protector (RIP) durchgeführt. Das Netzwerk und dessen Nutzung durch verschiedene Geräte wurden durch die Rhebo GmbH analysiert. Die daraus resultierenden Ergebnisse werden in diesem Dokument zur Verfügung gestellt.

Die Analyse basiert auf sämtlichen Aspekten Ethernet-basierter Kommunikation und den entsprechenden Geräten, die Nachrichten auf verschiedenen Netzwerkschichten senden, empfangen oder auf sonstige Weise in die Kommunikation involviert sind. Die Resultate beinhalten sowohl "normales" Verhalten (das an und für sich nicht bedrohlich, aber beachtenswert ist) als auch Verhalten, das möglicherweise bedenklich ist und gegebenenfalls ein Eingreifen erfordert. Diese Ergebnisse sind im Abschnitt "Präsentation der Ergebnisse" dargelegt.

Das Netzwerk wirkt insgesamt recht aufgeräumt und scheint im Vergleich zu ähnlichen Installationen gut strukturiert zu sein. Die Art der Kommunikation entspricht weitgehend dem Standard, mit einigen Ausnahmen. Die Übertragungsqualität im Netzwerk scheint immer wieder beeinträchtigt zu sein. Es wurden außerdem etliche Sicherheitsmängel identifiziert, denen dringend nachgegangen werden sollte.

Im Wesentlichen wurden potentielle Probleme in folgenden Bereichen identifiziert:

- verdächtige Kommunikation mit dem Internet
- verwundbare Switch-Firmware
- weitere möglicherweise verwundbare Software, Firmware und Betriebssysteme
- Infektion mit Schadsoftware
- nicht erreichbare Geräte
- nicht benötigte Protokolle
- auffälliges Zeitverhalten
- zeitweise erhöhte Antwortzeiten
- erhöhtes Aufkommen von Paketwiederholungen

Hinweise und Legende

Die obenstehende Zusammenfassung der Ergebnisse soll die in der nachfolgenden detaillierten Aufschlüsselung präsentierten Punkte nicht ersetzen oder deren Priorisierung abändern.

Dieses Dokument nutzt die folgenden Bewertungen:

Hohes Risiko für Stabilität bzw. Sicherheit des Netzwerks, bedarf sofortiger Behebung.

Warnung vor Bedrohung oder erhöhtem Risiko. Ggf. weitere Untersuchungen notwendig.

Keine ernsten Bedrohungen vorgefunden. Weiterführendes Monitoring wird empfohlen.

Keine Wertung möglich. Unvollständige Daten oder Analyse aus anderen Gründen nicht durchführbar.

RISSA Scorecard-Bewertungen

Rhebo hat Gesamtzustand und -qualität des Netzwerks auf Basis der von Rhebo Industrial Protector gelieferten Daten evaluiert. Die Analyse beinhaltet Einzelbetrachtungen und konkrete Handlungsempfehlungen. Darüber hinaus werden diese Ergebnisse anhand der folgenden Bewertungen in 5 Kategorien eingeordnet.

Netzwerkteilnehmer

Grund für die Bewertung	Was gemessen wurde
Die Art und Anzahl der der Netzwerkteilnehmer sowie deren Kommunikation entspricht weitgehend dem Standard.	Anzahl und Typ der Netzwerkteilnehmer sowie Kommunikationsmuster.

Sicherheitsrisiken

Grund für die Bewertung	Was gemessen wurde
Es wurden mögliche hohe Sicherheitsrisiken identifiziert, darunter Schadsoftware, verdächtige Aktivitäten und verwundbare Firmware.	Übersicht der Security-Maßnahmen. Offenheit des Netzes gegenüber externen Teilnehmern. Strategische Integration mit Monitoring-Lösungen (SIEM).

Produktivität und operationale Qualität

Grund für die Bewertung	Was gemessen wurde
Es wurden Hinweise auf Beeinträchtigungen der Netzwerkqualität gefunden, darunter regelmäßige Paketverluste und überlastete Übertragungskanäle.	Netzwerkqualität sowie Fehler, Warnungen usw., die die Echtzeit- und andere kritische Kommunikation beeinflussen können.

Continuous Improvement

Grund für die Bewertung

Es wurden keine Hinweise für die Integration der gesammelten Netzwerkdaten in ein weiterverarbeitendes System (z.B. SIEM) gefunden.

Was gemessen wurde

Daten des Steuernetzes werden in ein ERP, MES oder Big-Data-Projekt integriert, um für kontinuierliche Verbesserung der Qualität zu sorgen (Six Sigma, Kaizen, usw.)

Standardprozesse und Support

Grund für die Bewertung

Die Daten wurden ordnungsgemäß zur Verfügung gestellt. Die Ansprechpartner demonstrierten das nötige Fachwissen und waren kooperativ.

Was gemessen wurde

Fähigkeit, Rhebo bei der Integration und Analyse der Daten zu unterstützen. Standardisierte Prozesse, um ähnliche Geräte zu integrieren (z.B. IEC 62443, ISO/IEC 27002, Kapitel 8, 12, und 16)

Scorecard: Zusammenfassung der RISSA-Ergebnisse

Wert	Bedeutung
10	Der Zustand des Netzwerks gibt keinerlei Grund zu Beanstandungen bezüglich Sicherheit und Stabilität.
8	Hinsichtlich der Stabilität des Netzwerks gibt es nur wenig Verbesserungspotential. Die Sicherheit ist gewährleistet, u.U. mit kleineren Einschränkungen.
6	Die Stabilität des Netzwerks kann verbessert werden. Die Sicherheit ist grundsätzlich gewährleistet, allerdings sind Aktionen in geringem Umfang erforderlich.
4	Die Stabilität des Netzwerks kann deutlich verbessert werden. Es bestehen vereinzelte Mängel hinsichtlich der Sicherheit, die rascher Behebung bedürfen.
2	Der Zustand des Netzwerks weist deutliche Mängel sowohl hinsichtlich der Stabilität als auch der Sicherheit auf, eine akute Bedrohungslage ist jedoch unwahrscheinlich.
0	Die Sicherheit und Stabilität des Netzwerks sind unmittelbar bedroht.

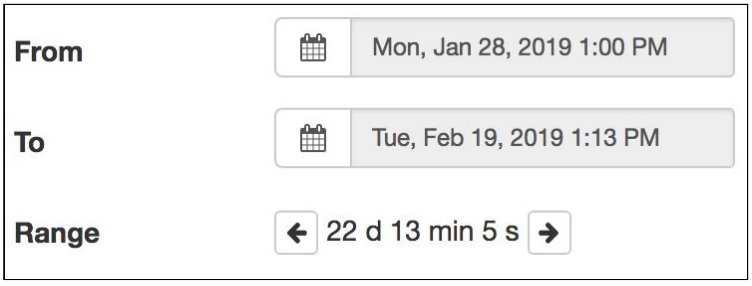
Rhebo-Installation

Rhebo stellt Betreibern von Steuernetzwerken eine Hardware-basierte oder virtualisierte Lösung zur Verfügung, mittels derer das Netzwerk überwacht und Sicherheits- sowie Produktivitätsrisiken minimiert werden können. Darüber hinaus bietet Rhebo zusammen mit Partnern Consulting und Dienstleistungen, die direkt mit den in diesem Report enthaltenen Befunden in Verbindung stehen.

Rhebo Industrial Protector untersucht den Verkehr des Steuernetzwerks, findet in diesem Anomalien, priorisiert potentielle Bedrohungen und stellt Daten für die forensische Analyse zur Verfügung. Das Produkt bietet spezifische Sichtbarkeit auf dem Gebiet industrieller Netzwerke und wird passiv und rückwirkungsfrei installiert. Der Rhebo Industrie 4.0 Stabilitäts- und Sicherheitsaudit (RISSA) basiert auf den Funktionalitäten des Industrial Protector.

Datensatz und Dauer der Aufzeichnung

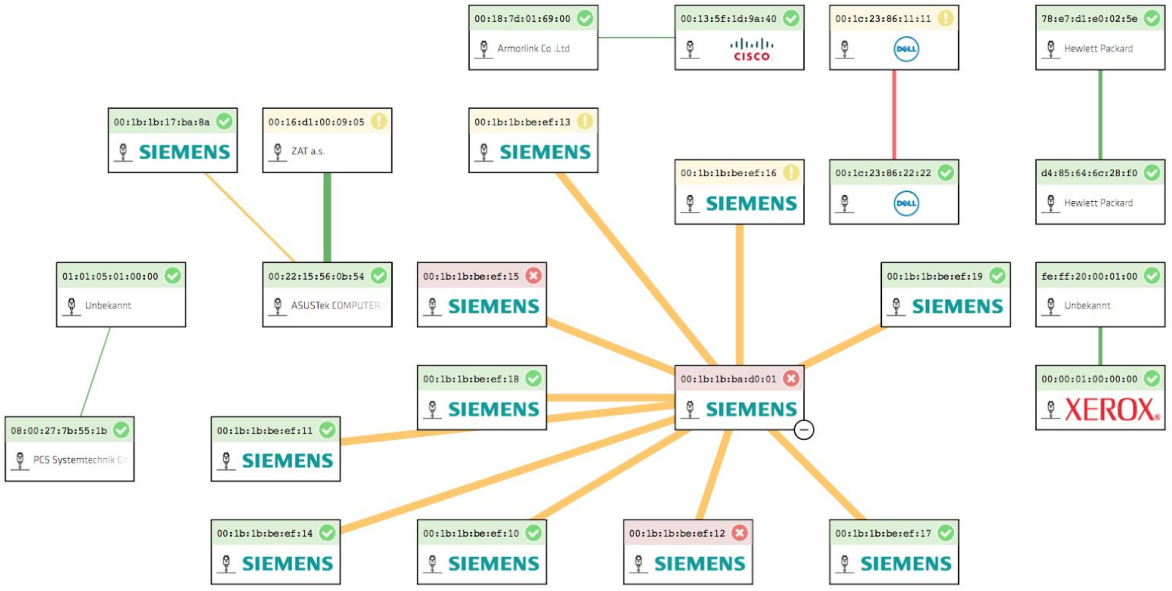
Rhebo Industrial Protector wurde im Netzwerk des Kunden am Standort Beispielhausen installiert. Die Aufzeichnungen erfolgten über 22 Tage in der Zeit vom 28.01.2019 bis zum 19.02.2019.



Infrastrukturaufbau und Statistiken

Gruppierung der Endgeräte

Die beobachteten Endgeräte teilen sich in 7 Cluster auf.



In Cluster 1 wird auf Layer 2 und Layer 3 kommuniziert. Es handelt sich hier vor allem um Kommunikation mittels IEC-60870-5-104 und Profinet, aber auch einiger anderer Protokolle wie ARP, NetBIOS und LLDP.

In den weiteren Clustern wird vor allem mittels Standard-IT-Protokollen kommuniziert.

Gerätehersteller (Auszug)

Hersteller	Anzahl
Siemens	29
Cisco	12
Hewlett Packard	2
Armorlink	1
Dell	1

Protokolle (Auszug)

Protokoll	Datenvolumen	Pakete
IEC60870-5-104	683 MB	4.001.175
Profinet	121 MB	1.581.031
ARP	31 MB	161.469
S7	751 KB	9.260
HSRP	191 KB	1.914

Präsentation der Ergebnisse

Verifizierung von Geräten und deren Kommunikation

Host 10.0.1.37: ungewöhnlicher Hersteller, Kommunikation ins Internet

Bei dem Host 10.0.1.37 handelt es sich um einen Kleincomputer des Typs Raspberry Pi. Dieser versendet 4 mal im Zeitraum der Aufzeichnungen offenbar verschlüsselte Daten an zwei Adressen im öffentlichen Adressraum des Internets. Die Server liegen im Adressbereich des ukrainischen Internet-Service-Providers Triolan. Es werden insgesamt 1,4 MB an Daten versendet.

Filter	Bewertung	Empfehlung
Host “10.0.1.37”	✕	Es sollte dringend geprüft werden, ob das Gerät bzw. die Kommunikation erwünscht ist.

Gerät sw-1020-a: verwundbarer Switch

Der Switch a0:b3:cc:27:11:1e des Typs HP ProCurve J9279A 2510G-24 läuft mit der Firmware-Version Y.11.12, für die eine schwerwiegende Sicherheitslücke besteht. Diese ermöglicht es einem Angreifer im lokalen Netz, Informationen aus dem Gerät auszulesen.

Der Hersteller hat bereits im Juli 2013 die fehlerbereinigte Version Y.11.38 zur Verfügung gestellt.

Mehr Informationen hierzu unter:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-7270
- https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c03819065

Host	Impact	Risk Score	Notifications	Vendor	Device Type	Firmware Version
:19	67	0.0		Hewlett Packard	BRIDGE	ProCurve J9279A Switch 2510G-24, revision Y.11.12, ROM N.10.02 (/sw/code/build/cod(cod11))

Filter	Bewertung	Empfehlung

Gerät “a0:b3:cc:27:11:1e”	✗	Die Firmware des Geräts sollte baldmöglichst aktualisiert werden.

Host 10.0.2.43: verwundbare Software

Der Host 10.0.2.43 nutzt UDP-Port 22350. Dabei handelt es sich offenbar um die Software Wibu-Systems AG CodeMeter, für die in der vorliegenden Version 4.30c eine schwere Sicherheitslücke vorliegt, die es einem Angreifer im lokalen Netz erlaubt, den Dienst zum Absturz zu bringen.

Mehr Informationen hierzu unter:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4057

Filter	Bewertung	Empfehlung
Protokoll “CodeMeter”	✗	Es ist zu prüfen, ob es sich um die vermutete Software handelt. Ggf. sollte diese baldmöglichst aktualisiert werden.

Host 10.0.1.55: verwundbares Betriebssystem

Der Host 10.0.1.55 läuft unter Microsoft Windows 2008 Server R2 zu laufen. Für diese Betriebssystemversion ist eine Vielzahl von zum Teil hochkritischen Sicherheitslücken bekannt.

```
▶ GET /cgi/port_usage?LAST_PORT=48&NUM_PORTS=26 HTTP/1.
  Cache-Control: no-cache\r\n
  Pragma: no-cache\r\n
  User-Agent: Mozilla/4.0 (Windows Server 2008 R2 6.1)
```

Mehr Informationen hierzu unter:

- https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-11366/version_id-91068/Microsoft-Windows-Server-2008-R2.html

Filter	Bewertung	Empfehlung

Host “10.0.1.55”		Das Betriebssystem sollte baldmöglichst aktualisiert werden.

Oracle JDK 1.8.0: verwundbare Java-Implementierung

Der Host 10.0.1.3 nutzt offenbar die Java-Version 1.8.0, für die mehrere, zum Teil schwerwiegende Sicherheitslücken bestehen, die es einem Angreifer ermöglichen, die Kontrolle über das System zu übernehmen.

Mehr Informationen hierzu finden sich unter:

https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19116/version_id-168996/year-2014/Oracle-JDK-1.8.0.html

Filter	Bewertung	Empfehlung
Protokoll “HTTP”, Host “10.0.1.3”		Der Wechsel auf eine aktuelle Implementierung sollte geprüft werden.

TCP-Port 2080: Befall mit Schadsoftware

Zwischen den Hosts 10.0.1.40 und 10.0.1.46 werden binäre Daten über TCP-Port 2080 ausgetauscht.

Der Port wird vom Trojaner Backdoor.Tjserv benutzt, der Windows-Systeme befällt und mit dessen Hilfe ein Angreifer unerlaubten Zugriff auf ein System erhalten kann. Ein sicheres Zeichen für die Infektion ist die Existenz des Registry-Schlüssels “HKEY_CURRENT_USER\Software\tjservers”.

Mehr Informationen hierzu finden sich unter:

https://www.symantec.com/security-center/writeup/2004-111117-0241-99

Filter	Bewertung	Empfehlung
Protokoll “CUSTOM: TCP-Port 2080”		Es sollte festgestellt werden, ob die Kommunikation plausibel ist. Ggf. sollten die Hosts einem Virus-Scan unterzogen werden.

Unsicheres Protokoll: SMBv1

Der Host 10.0.1.15 kommuniziert über SMB. Dabei kommt SMB in der veralteten Variante 1 zum Einsatz. SMBv1 wurde 2006 durch eine neuere Version abgelöst und wird seitdem nicht mehr gepflegt. Aktuell sind über 500 zum Teil hochkritische Schwachstellen bekannt, die SMBv1 zugeordnet werden können.

SMBv1 wird weiterhin häufig über den NT LAN Manager authentifiziert. Damit besteht die Möglichkeit, dass ein lokaler Angreifer Zugriff auf die Passwort-Hashes der Benutzer erhält. Mehr Informationen hierzu unter:

https://pentest.blog/what-is-llmnr-wpad-and-how-to-abuse-them-during-pentest/

Diese Hashes können von aktueller Hardware in wenigen Stunden geknackt werden, so dass der Angreifer sich im Nachhinein auf den entsprechenden Windows-Hosts als privilegierter Benutzer einloggen könnte:

https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

Darüber hinaus sind SMB-Relay-Attacken möglich:

https://cqureacademy.com/blog/penetration-testing/smb-relay-attack

Filter	Bewertung	Empfehlung
Protokoll “SMB”	✕	Die SMB-Services sollte auf eine aktuelle Version geupdated werden. Der Umstieg auf eine sichere Authentifizierungs-Variante wie Kerberos sollte in Erwägung gezogen werden.

Mögliches ARP-Spoofing

Während des Überwachungszeitraums wurden 2 sogenannte Gratuitous-ARP-Request gemeldet. Dies bedeutet, dass ein Gerät per ARP nach seiner eigenen IP-Adresse fragt. Das Protokoll ARP dient zur Zuordnung von MAC- zu IP-Adressen. Auch Anfragen enthalten die eigene MAC- und IP-Adresse des jeweiligen Hosts. Diese Zuordnung wird von den jeweils empfangenden Hosts ohne weitere Prüfung übernommen, so dass ein potentieller Angreifer von einem Gerät, das unter seiner Kontrolle steht, jede beliebige IP-Adresse vortäuschen kann. Dieses sogenannte ARP-Spoofing ermöglicht Man-In-The-Middle-Angriffe, bei dem

der Angreifer beliebigen Verkehr im Netzwerk mitlesen kann. Gratuitous-ARP-Anfragen sind ein Hinweis auf ARP-Spoofing.

Es handelt sich um diese Geräte:

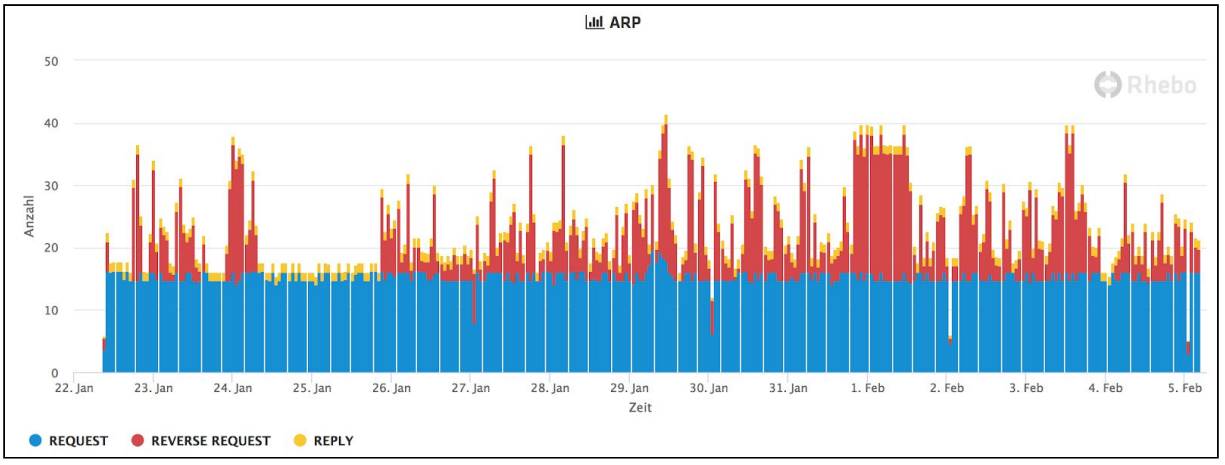
- ee:fc:01:23:22:41 (gibt die IP-Adresse 10.0.1.47 an)
- ee:fc:01:25:01:07 (gibt die IP-Adresse 10.0.1.198 an)

Filter	Bewertung	Empfehlung
Meldungstyp “Gratuitous-ARP-Anfrage”	—	Es sollte geprüft werden, ob von diesen Geräten bösartige Aktivität ausgeht.

Große, ungleich verteilte Menge von ARP Reverse Requests

Während des Überwachungszeitraums wurden sehr viele ARP Reverse Requests (RARP) registriert. Die zeitliche Verteilung dieser Requests ist sehr ungleichmäßig und daher auffällig. ARP Reverse Requests werden verwendet um eine Layer-3-Adresse (IP-Adresse) für einen Layer-2-Host (MAC-Adresse) zu beziehen, und werden heute eher selten verwendet. Die Funktionalität wird stattdessen über DHCP realisiert.

Die ungleiche Verteilung kann auf den Neustart oder Neukonfiguration von bestimmten Gerätetypen zurückgeführt werden. Es besteht aber auch die Möglichkeit des so genannten ARP-Stuffing. Diese Methode weist Geräten eine IP-Adresse zu, ohne DHCP zu verwenden. ARP-Stuffing ist anfällig für eine Reihe von Angriffen und in den meisten Fällen unerwünscht.



Filter	Bewertung	Empfehlung

Protokoll “ARP”/Funktionen	—	Identifikation der betroffenen Geräte. Ggf. Update von Geräten und Konfiguration zur Verwendung von DHCP statt RARP. Falls nötig: Abschaltung von RARP/ARP-Stuffing.

Potentieller ICMP-Redirect-Angriff

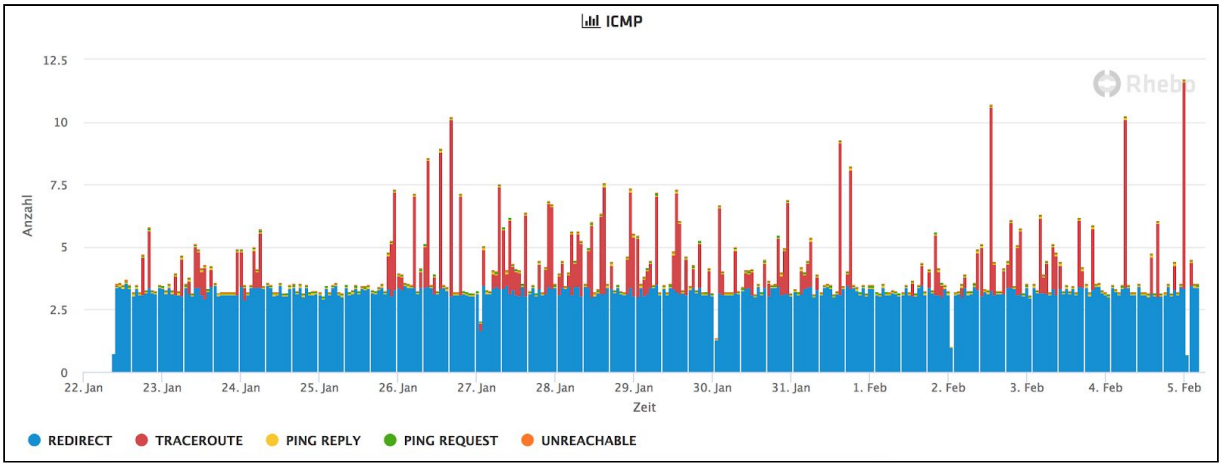
Die folgenden IP-Adressen versenden ICMP-Redirect-Nachrichten im Netzwerk:

- 10.0.1.240
- 10.0.1.242

ICMP-Redirects fügen einen neuen, dynamischen Eintrag in der Routingtabelle des Zielhosts hinzu, der zeitlich unbegrenzt Gültigkeit hat. (Der neue Zielrouter muss allerdings im selben Subnetz liegen.) Fehlerhafte oder bewusst gefälschte ICMP-Redirects können in Form einer ICMP-Redirect-Attacke das Routing im Netzwerk negativ beeinflussen. Ein Angreifer kann so beliebige Datenflüsse umleiten.

Betroffene Zielhosts, deren Routing-Tabellen verändert wurden:

- 10.0.1.33
- 10.0.1.57
- 10.0.1.144
- 10.0.1.201



Filter	Bewertung	Empfehlung

Protokoll “ICMP”	—	Prüfung, ob eine legitime Verwendung von ICMP-Redirects vorliegt, und Prüfung des Routings zur Vermeidung von Redirects.

Unsicheres Protokoll: Telnet

Der Host 10.0.1.19 baute am 21.01.2019 07:41 eine Telnet-Verbindung zum Host 10.0.1.11 auf.

Das Protokoll ist unverschlüsselt und bietet einem lokalen Angreifer die Möglichkeit, sensible Daten inklusive eventuell übertragener Passwörter einzusehen. Logindaten für einen Administrator-Account sind in den aufgezeichneten Daten im Klartext enthalten.

Filter	Bewertung	Empfehlung
Protokoll “Telnet”	—	Wechsel auf eine sichere, verschlüsselte Alternative wie SSH. Ggf. ist dazu ein Firmware-Update erforderlich.

Nicht erreichbare Hosts

Die folgenden Hosts sind zumindest zeitweise nicht im Netzwerk erreichbar:

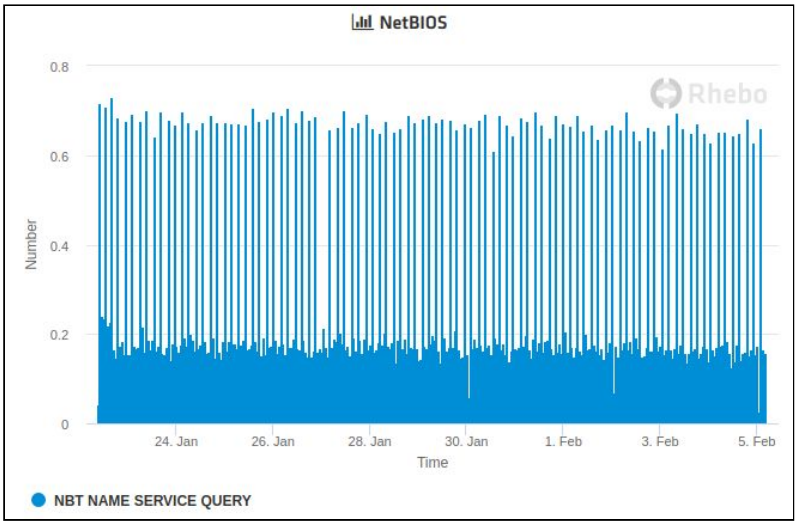
- 10.0.1.44
- 10.0.1.130
- 10.0.1.135

Dies ist erkennbar durch entsprechende ICMP-Unreachable-Meldungen.

Filter	Bewertung	Empfehlung
Protokoll “ICMP”	—	Es sollte geprüft werden, ob dieses Verhalten plausibel ist. Ggf. muss die Konfiguration der anfragenden Hosts angepasst werden.

Zyklische Spitzen in der NetBIOS-Kommunikation

In der NetBIOS-Kommunikation sind deutliche Spitzen von Name Service Queries zu erkennen. Diese treten etwa alle 3½ Stunden und während des gesamten Überwachungszeitraums auf. Insgesamt nutzen 32 Hosts das Protokoll NetBIOS, allerdings lässt sich der Host 10.0.1.12 als Quelle für die Spitzen identifizieren. Anscheinend scannt dieser Host zyklisch das Netzwerk nach anderen Teilnehmern.



Filter	Bewertung	Empfehlung
Funktionen “NetBIOS”	—	Verifikation des Verhaltens des Hostes, und Prüfung, ob es sich um erwünschtes Verhalten handelt.

Kurzzeitig erhöhte Datenrate

Am 12.02.2019 gegen 7:55 erhöht sich für einen kurzen Zeitraum der Datendurchsatz im Netzwerk um fast 200%. Dies betrifft vor allem das Protokoll IEC-60870-5-104, bei dem in diesem Zeitraum zudem etliche neue Funktionen zum ersten Mal auftreten.

Ebenfalls zu dieser Zeit tauchen verstärkt Qualitätsprobleme auf, wie Überschreitungen der Paketumlaufzeit, doppelte TCP-Acknowledgements, Paketwiederholungen und ungültige Sequenznummern.

Vermutlich wurden in diesem Zeitraum Wartungsarbeiten durchgeführt bzw. Systeme neu gestartet.

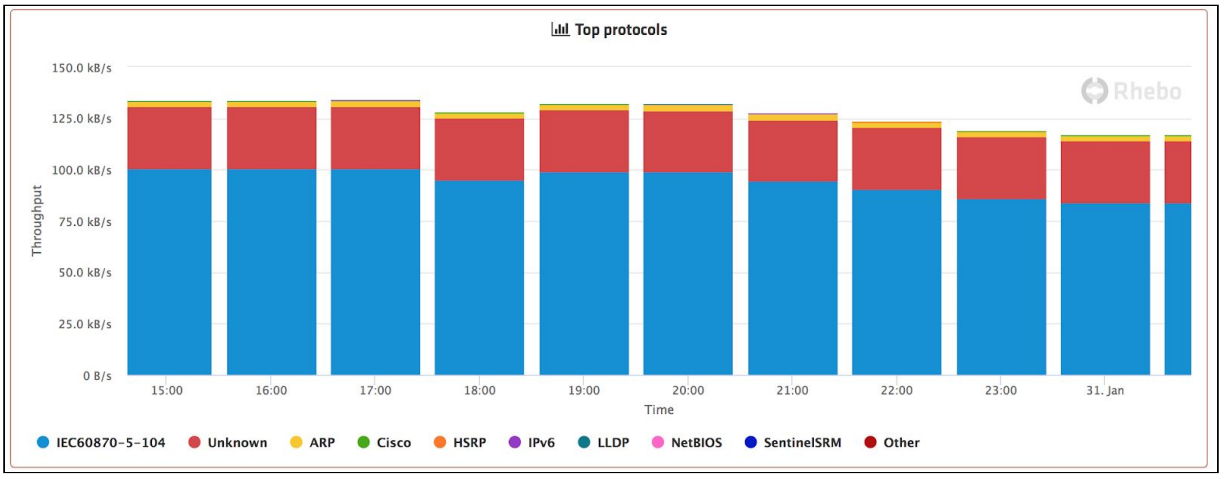
Filter	Bewertung	Empfehlung

Ansicht “Protokolle” bzw. Ansicht “Meldungen”, Meldungsklasse “Diagnose”	—	Es sollte geprüft werden, ob die Lastspitze und die damit verbundenen Phänomene plausibel sind.

Host 10.0.40.43: Scan-Aktivität

Der Host 10.0.40.43 scannt offenbar das Netzwerk mittels TCP. Es erfolgen Verbindungsversuche auf Port 2404, der für IEC-60870-5-104 genutzt wird. Diese bleiben zum Teil unbeantwortet.

Die Scan-Pakete und die darauf erfolgenden Antworten (hier rot dargestellt) machen einen beträchtlichen Teil der gesamten Netzlast aus: Während des Zeitraums der Aufzeichnungen sind es fast 25%.



Filter	Bewertung	Empfehlung
Meldungstyp “Adress-Scan”	—	Es sollte geprüft werden, ob die Scan-Aktivität plausibel bzw. erwünscht ist. Wenn möglich, sollten die Anfragen unterbunden bzw. die Frequenz verringert werden.

Host 10.0.1.80: Aussetzen der Kommunikation

Der Host 10.0.1.80, eine Steuerung des Herstellers ABB, kommuniziert fast durchgängig, allerdings ist eine längere Pause der Aktivitäten festzustellen, und zwar vom 07.02.2019 um

07:00 Uhr bis zum 09.02.2019 um 12:00 Uhr. In dieser Zeit wird anfangs kaum und später überhaupt nicht mehr kommuniziert.

Filter	Bewertung	Empfehlung
Host “10.0.1.80”	—	Es sollte geprüft werden, ob die Lücke plausibel ist.

Host 10.0.1.98: TCP-Fenster mit Größe 0.

Der Host 10.0.1.98 meldet am 12.02. um 14:40 ein TCP-Fenster mit Größe 0. Diese Meldung bedeutet, dass das jeweilige Gerät zu diesem Zeitpunkt keine Daten auf der entsprechenden TCP-Verbindung empfangen kann. Ein Grund hierfür kann sein, dass das Gerät überlastet ist oder die jeweilige Anwendung zum Beispiel in einer Endlosschleife hängt.

Filter	Bewertung	Empfehlung
Meldungstyp “TCP-Fenstergröße 0”	—	Die Firmware bzw. das Betriebssystem des betroffenen Geräts sollte aktualisiert werden.

Host 10.0.1.31: Auffällige TCP-Implementierung

Der Host 10.0.1.31 sendet minütlich TCP-ACK-Pakete zu scheinbar zufälligen IP-Adressen, ohne dass eine entsprechende Verbindung aufgebaut wurde. Offenbar liegt eine fehlerhafte TCP-Implementierung vor.

Filter	Bewertung	Empfehlung
Host “10.0.1.31”	—	Die Firmware bzw. das Betriebssystem des betroffenen Geräts sollte aktualisiert werden.

Isoliertes Gerät 00:19:0b:07:41:3d

Das Gerät 00:19:0b:07:41:3d scheint im Netzwerk isoliert zu sein. Es sendet nur ARP-Anfragen, auf die keine Antworten folgen, sowie einmalig ein TCP-SYN-Paket an den Host 10.0.22.21, das allerdings ebenfalls nicht beantwortet wird.

Filter	Bewertung	Empfehlung
Meldungstyp “00:19:0b:07:41:3d”	—	Es sollte geprüft werden, ob das Gerät im Netzwerk benötigt wird bzw. weshalb es in seiner Kommunikation eingeschränkt ist.

Nicht benötigtes Protokoll Web Services Discovery

Zwei Hosts nutzen das Protokoll Web Services Discovery:

- 10.0.1.17
- 10.0.1.19

Dies wird vermutlich für die Grundfunktion des Netzwerks nicht benötigt. Es werden lediglich Multicast-Pakete versendet, ohne dass darauf Antworten erfolgen.

Nicht benötigte Protokolle stellen potentielle Angriffsvektoren dar und sollten daher abgeschaltet werden. Dieses Protokoll ist auch immer wieder von Sicherheitslücken betroffen, so dass diese Empfehlung in besonderem Maße gilt.

Filter	Bewertung	Empfehlung
Protokoll “Web Services Discovery”	—	Es ist zu prüfen, ob das Protokoll im Netzwerk erforderlich bzw. erwünscht ist. Ansonsten ist die Nutzung per Konfiguration zu unterbinden.

Netzwerkqualität und Diagnose

Auffälligkeiten im Zeitverhalten zyklischer Nachrichten

Für mehrere Hosts aus den Subnetzen 10.0.2.0/24 und 10.0.4.0/24 werden wiederholt Probleme bei der Kommunikation mittels zyklischer IEC-60870-5-104-Nachrichten festgestellt. Folgende Auffälligkeiten sind zu verzeichnen:

- zyklische Nachricht zu früh
- zyklische Nachricht zu spät
- zyklische Nachricht fehlt

Dies deutet darauf hin, dass es in diesem Zeitraum wiederholt zu erhöhten Latenzen im Netzwerk kam. Eine Ursache kann fehlerhaftes Netzwerk-Equipment wie Kabel oder Switches sein. Aber auch Fehlkonfigurationen der entsprechenden Geräte sowie Softwarefehler sind denkbar.

Die Meldungen treten häufiger auf als in vergleichbaren Umgebungen üblicherweise beobachtet wird.

Filter	Bewertung	Empfehlung
Meldungstypen “Zyklische Nachricht zu früh”, “Zyklische Nachricht zu spät” und “Zyklische Nachricht fehlt”	—	Software und Konfiguration der betroffenen Endgeräte sowie Übertragungskanäle ggf. inkl. Logs entsprechender Switches überprüfen. Die entsprechenden Meldungen überwachen. Regelmäßig die Häufigkeit überprüfen.

Überschreitungen der Paketumlaufzeit

Etliche Verbindungen sind immer wieder von Überschreitungen der Paketumlaufzeit betroffen. Dies bedeutet, dass die auf der jeweiligen Verbindung beobachteten durchschnittlichen Antwortzeiten zu gewissen Zeitpunkten deutlich überschritten werden. Dies ist ein Hinweis darauf, dass zeitweise die Übertragungsqualität auf dem jeweiligen Netzabschnitt gemindert war. Die Meldungen stehen jedoch nicht im zeitlichen Zusammenhang mit Lastspitzen.

Betroffen sind hiervon ausschließlich IEC-60870-5-104-Verbindungen und Hosts des Subnetzes 10.0.2.0/24.

Filter	Bewertung	Empfehlung
Meldungstyp “Überschreitung der Paketumlaufzeit”	—	Es ist zu prüfen, ob die Zeitverletzungen negative Auswirkungen auf die Funktion des Anlage haben. Eventuell sind einzelne Komponenten überlastet. Netzwerk-Equipment wie Kabel und Switches sollte überprüft werden.

TCP-Verkehr nach Reset

Einige Hosts senden TCP-Pakete, nachdem auf der entsprechenden Verbindung ein Reset beobachtet wurde. Betroffen ist ausschließlich das Protokoll IEC-60870-5-104.

Ein solches Reset sollte die Verbindung unmittelbar und ohne Bestätigung beenden. Wird trotzdem weiterhin Verkehr gesendet, wurde das Reset entweder nicht korrekt empfangen oder es liegt eine fehlerhafte TCP-Implementierung im empfangenden Endpunkt vor.

Filter	Bewertung	Empfehlung
Meldungstyp “TCP-Verkehr nach Reset”	—	Die Software der betroffenen Endgeräte und die Auslastung der Übertragungsstrecken sollte überprüft werden. Die entsprechenden Meldungen überwachen. Regelmäßig die Häufigkeit überprüfen.

TCP-Übertragungswiederholung

Von einigen Hosts wurden während der Aufzeichnungen TCP-Übertragungswiederholungen beobachtet. Betroffen ist vor allem das Protokoll IEC-60870-5-104.

Ein gehäuftes Auftreten solcher Übertragungswiederholungen ist oft ein Zeichen für fehlerhafte Komponenten wie Ethernet-Kabel und Switches.

Die Meldungen treten wesentlich häufiger auf als in vergleichbaren Netzwerken üblicherweise beobachtet wird.

Filter	Bewertung	Empfehlung
Meldungstyp “TCP-Übertragungswiederholung”	—	Die entsprechenden Meldungen überwachen. Regelmäßig die Häufigkeit überprüfen. Auslastung der Übertragungskanäle beachten.

Nächste Schritte

Die oben beschriebenen Sachverhalte sollten vom Kunden wie empfohlen analysiert werden. Rhebo kann dabei unterstützen. Es wird ein Gesprächstermin vereinbart, an dem neben Rhebo auch technisches sowie Management-Personal des Kunden teilnehmen sollte. Dieses ist in der RISSA-Dienstleistung enthalten.

Es wird gebeten, Rhebo zu kontaktieren, um Informationen zu einer eventuellen flächendeckenden Installation und/oder Betreuung durch einen Systemintegrator zu erhalten.

Schritt	Beschreibung	Zeitrahmen
Koordinierung der erforderlichen Maßnahmen	Workshop zwischen technischem Personal und Rhebo	15.03.2019
Vierteljährliches RISSA	Analyse der im Quartal angefallenen Daten des Steuernetzwerks	Mai 2019

Virtual Machine

Compact Controller

Controller