

Memorandum

Thema:	Glossar zur IT-Sicherheit
Datum:	20.08.2018
Ort:	Dresden und Seligenstadt
Von:	Brock Schomberg
An:	öffentlich

Inhalt

IT-Sicherheit / Datenschutz	3
Active Directory	4
Angriffsmethoden	4
APT	4
Brute Force	4
DDoS	5
Man-in-the-Middle	5
Phishing	5
Ransom (dt. Lösegeld)	6
Social Engineering	6
Authentifizierung / Autorisierung / Authentizität	6
BDEW Whitepaper	7
BSI	7
Cloud	7
Härtung	8
Intrusion Detection	8
IPsec	8
ISMS / Kundenanforderung	9
Kritische Infrastruktur	9
PKI	9
Protokolle - Anwendungsebene	10
FTP/SFTP/FTPS	10
HTTP/HTTPS	10
Radius	10
Protokolle - Netzwerkebene	10
DHP	10
HSR	10
MRP	11
PRP	11
RSTP	11
RSTP Enhanced	11
SHP	11
RBAC	11
SAM	11
Sicherheitsmeldung	12
SIEM	12
SNMP	13
SSL	13
Standards	13
TLS	13
Verschlüsselung	14
VPN	15
VLAN	15

Zertifikat	15
Zertifikatemanagement	16

IT-Sicherheit / Datenschutz

IT-Sicherheit,

- auf Englisch Cybersecurity,
- auf Deutsch Cyber Security,

umfasst alle Maßnahmen, die darauf abzielen, Informationen

- verfügbar,
- richtig und
- vertraulich

zu halten.

Datenschutz,

- auf Englisch data privacy, oder protection of data privacy,
- auf Englisch auch GDPR (global data protection regulation)
- auf Deutsch auch EU-DSGVO (Datenschutzgrundverordnung)

umfasst alle Maßnahmen, die darauf abzielen,

- natürliche Personen vor Missbrauch ihrer Daten zu schützen und
- den Verkehr personenbezogener Daten zu regeln.

Active Directory

Das ist ein Leistungsangebot (Server und zugehöriges Kommunikationsprotokoll) von Microsoft aus dem Bereich der Büro-IT. Ein AD-Server nimmt einen Benutzernamen und ein Passwort entgegen und antwortet im weitesten Sinne:

1. Die identifizierte Person ist bekannt/unbekannt.
2. Die identifizierte Person hat das folgende Benutzerprofil.
3. Die identifizierte Person hat Zugriff auf die folgenden Systemressourcen.

Viele unserer Kunden (und wir ja auch) haben einen AD-Server in ihrer Büroumgebung etabliert. Darum erscheint es naheliegend, diese Einrichtung für die Authentifizierung (siehe dort) im operativen Betrieb von Schaltanlagen zu verwenden. Das erfordert eine

1. Verbindung unserer Stationsnetze mit dem Firmennetz. – Wir planen den Einsatz unseres SAM (siehe dort) als AD-Gateway.
2. Abbildung der Benutzerrechte (für Schutz und Steuerung) in einem hierfür nicht gedachten AD-Server. – Wir planen, die Benutzerrechte in SAT (siehe dort) zu definieren und in die Steuergeräte zu laden.

Angriffsmethoden

APT

Ein **Advanced Persistent Threat** ist ein Angriffstyp mit individuell zugeschnittener Methode. Hierbei wird eine bekannte Schwachstelle in einer Systemkomponente ausgenutzt, um

1. Kenntnisse über das System zu sammeln,
2. individuell entwickelte, feindliche Software auf den entdeckten Komponenten zu platzieren und
3. deren Entfernung durch „Ausweichen auf andere Rechner“ zu verhindern.

Ziele sind, wie bei allen Angriffen,

1. Spionage,
2. Funktionsunterbrechung und
3. Funktionsfälschung.

Der Aufwand für die Durchführung eines APT ist so groß, dass er im Allgemeinen nur Geheimdiensten zugetraut wird. Die Detektierung ist schwer, weil der Angriff individuell gestaltet ist und keinem bekannten Muster folgt. Der Deutsche Bundestag wurde 2015 mit einem APT angegriffen.

Brute Force

Das ist ein Angriffstyp, bei dem nicht eine Person, sondern eine Software, die vorgibt eine Person zu sein, einen Benutzernamen verwendet und dann über einen längeren Zeitraum alle möglichen Passworte ausprobiert.

Detektion: tricky. Das ist eigentlich nur mit einem SIEM (siehe dort) möglich.

Gegenmaßnahme: Hier muss ein Limit (maximale Anzahl fehlgeschlagener Anmeldungen eines Benutzers in einem gegebenen Zeitraum) definiert werden. Wird das Limit überschritten, dann kann

1. eine Sicherheitsmeldung abgesetzt und.
2. das Konto des betreffenden Benutzers gesperrt werden.

DDoS

Ein **Distributed Denial of Service** ist ein Angriffstyp, bei dem eine Software mit den folgenden Funktionen zum Einsatz kommt.

1. Die Software installiert sich (feindlich) auf maximal vielen Rechnern im Internet.
2. Sie hält (ggf. über einen längeren Zeitraum) Stille, sodass sie nicht auffällt.
3. Zu einem definierten Zeitpunkt richtet die Software von all ihren Installationen gleichzeitig Anfragen an einen Server (Fokus auf Webseiten), sodass er unter der Last der Anfragen seine Arbeit einstellt.

Gegenmaßnahme: Die betroffene Kommunikationsschnittstelle muss sehr sauber programmiert, getestet und dokumentiert sein. Ein zeitweises Versagen unter einer DDoS-Attacke kann toleriert werden, wenn es gemäß einer abgestimmten Spezifikation verläuft.

Unser Schutz wurde hierzu von Amrion erfolgreich getestet.

Man-in-the-Middle

Das ist ein Angriffstyp, wobei die Kommunikation zwischen zwei oder mehreren Kommunikationspartnern abgehört und ggf. gefälscht wird.

Ein Beispiel hierfür war ein Angriff Ende 2016 auf eine Schaltanlage der Ukraine. Hier wurde eine feindliche 104-Implementierung eingebracht. Sie hatte die folgenden Funktionen.

1. Langfristiger Mitschrieb der 104-Kommunikation
2. Rückschluss von der Kommunikation auf die Primärtechnik
3. Absendung von Schaltbefehlen

Gegenmaßnahmen: Verschlüsselte Kommunikation und Härtung (siehe dort)

Phishing

Hierunter versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten Internet-Benutzers zu unbedachten Handlungen zu verleiten, die auf Identitätsdiebstahl hinauslaufen.

Hier ein paar Beispiele aus meiner privaten Mail. Ich kenne keine einzige der aufgeführten Personen.

<input type="checkbox"/>	Katharina Meier	Hallo, Dringende Antwort benoetigt!	14.05.2018	5,16 KB
<input type="checkbox"/>	Christina Meyer	Vorsicht! Pressemitteilung! Von Notar Getestet!	13.05.2018	7,95 KB
<input type="checkbox"/>	Ihre Smartwatch	Erster sein und trendige Smartwatch sichern für 7x stern lesen, lieber Leser!	13.05.2018	31,37 KB
<input type="checkbox"/>	Ole Neumann	Strafe	13.05.2018	6,69 KB
<input type="checkbox"/>	Melina Schaefer	Mein Anruf	12.05.2018	8,12 KB
<input type="checkbox"/>	Lea Lang	(1) NEUE Nachricht...	12.05.2018	10,27 KB
<input type="checkbox"/>	Finja Frank	Rechnungsnummer 29391	12.05.2018	8,56 KB
<input type="checkbox"/>	Antonia Hartmann	Ihr Einkauf war erfolgreich! Rechnung 09.05.2018	11.05.2018	8,81 KB
<input type="checkbox"/>	Helena Schulte	Meine letzte E-Mail	11.05.2018	7,69 KB

Die effektivste Gegenmaßnahme ist auf nichts zu klicken, was man

- nicht kennt,
- nicht versteht oder
- nicht erbeten hat.

Ransom (dt. Lösegeld)

Hierunter versteht man die Einbringung einer feindlichen Software, welche

1. nach Betriebsdaten sucht,
2. diese kopiert, verschlüsselt und mit einem Passwort sichert,
3. den originalen Datenbestand löscht und so
4. die Arbeitsfähigkeit des befallenen Rechners beendet.

In der Folge wird dem Betreiber ein Angebot für den Erwerb des Passwortes unterbreitet. Hiermit kann die Arbeitsfähigkeit wieder hergestellt werden.

Abwehrmaßnahmen:

1. Keine USB-Sticks und nicht auf irgendwelche Links klicken
2. Regelmäßiges Backup
3. Vorhaltung Backup-Rechner

Social Engineering

Unter Social Engineering (dt.: soziale Manipulation) versteht man den Versuch einen Benutzer durch eine persönliche/telefonische Ansprache (etwa mit einer Bitte um unbürokratische Hilfestellung) zu unbedachten Handlungen, etwa

1. Preisgabe eines Passwortes,
2. Einrichtung eines Benutzerkontos oder
3. Freigabe einer Zahlung

zu verleiten.

Abwehrmaßnahme: zweifelsfreie Klarstellung von Identität und Berechtigung des Anfragenden.

Authentifizierung / Autorisierung / Authentizität

Zuerst die Eselsbrücke:

1. Authentifizierung beantwortet die Frage: „Kennst Du mich?“
2. Autorisierung beantwortet die Frage: „Darf ich das?“
3. Authentizität herrscht nach der zweifelsfreien Feststellung der Identität.

Die folgenden Abläufe sind in unseren Systemen denkbar:

1. Alles lokal – hierbei
 - a. meldet sich ein Benutzer an einem Steuergerät an.
 - b. *Authentifizierung*: Jetzt verifiziert das Steuergerät in seinem lokalen Speicher (gefüllt von SAT) Benutzernamen und Passwort.
 - c. *Autorisierung*: Jetzt weist das Steuergerät aus seinem lokalen Speicher dem Benutzer eine Rolle und seine Rechte zu.
2. Anfrage an SAM – hierbei
 - a. meldet sich ein Benutzer an einem Steuergerät an.
 - b. *Authentifizierung*: Jetzt wendet sich das Steuergerät an SAM und bittet um Authentifizierung des Benutzers „Schomberg“ mit Passwort „swordfish“.
 - c. SAM antwortet „Den kenn ich und er ist ein Schaltberechtigter.“
 - d. *Authorisierung*: Jetzt weist das Steuergerät aus seinem lokalen Speicher dem Benutzer eine Rolle und seine Rechte zu.
3. SAM als Gateway zum Active Directory (zukünftig) – hierbei
 - a. meldet sich ein Benutzer an einem Steuergerät an.
 - b. *Authentifizierung*: Jetzt wendet sich das Steuergerät an SAM und bittet um Authentifizierung des Benutzers „Schomberg“ mit Passwort „swordfish“.

- c. SAM leitet die Anfrage aus der Station zum externen Active Directory weiter.
- d. Das Active Directory antwortet „Den kenn ich und er ist ein Schaltberechtigter.“
- e. SAM leitet die Antwort an das Steuergerät weiter.
- f. *Authorisierung*: Jetzt weist das Steuergerät aus seinem lokalen Speicher dem Benutzer eine Rolle und seine Rechte zu.

BDEW Whitepaper

Der **Bund der Deutschen Elektrizitäts- und Wasserwirtschaft** hat eine Liste von 217 Anforderungen zur IT-Sicherheit herausgegeben, die sich an

- 1. Produkte,
- 2. Systeme und
- 3. Lieferorganisationen

richten.

Da diese Anforderungen von einem herstellerneutralen Dachverband zusammengetragen wurden, können Sie als Standard angesehen werden. Wir haben die Anforderungen für

- 1. P30
- 2. P40
- 3. Saitel DR
- 4. C264
- 5. T300
- 6. Pacis
- 7. Clear SCADA
- 8. S30
- 9. Eberle Reg-D

beantwortet und nennen das Ergebnis ein BDEW-Profil. Das ist ein schöner Teil unserer Produktdokumentation.

BSI

Das **Bundesamt für Sicherheit in der Informationstechnik** (www.bsi.bund.de) ist eine zum Innenministerium gehörende Behörde, die Betreiber kritischer Infrastrukturen (siehe dort) mit Hinblick auf IT-Sicherheit

- 1. kennt,
- 2. berät,
- 3. anweist,
- 4. auditiert und
- 5. ggf. sanktioniert.

Das ist dieselbe Funktion, die die Bankenaufsicht für den Finanzsektor erfüllt.

Cloud

Das ist eine Wortschöpfung für ein Leistungsangebot in den Bereichen

- 1. Dateiablage,
- 2. Archivierung,
- 3. Backup,
- 4. Integration mit Produkten (Autonavagation, Schutzzeinstellungen etc.) und
- 5. allgemeinerer Funktionen (Filterung, Aufbereitung, Bearbeitung, Hinterherschmeißung etc.).

Prominente Beispiele sind die

1. Mindsphere (Bewusstseinskugel) bei Siemens und die
2. Box (Schachtel) bei uns.

Kritikpunkt kommt aus dem Bereich der IT-Sicherheit:

1. Wer ist verantwortlich für die Datenablage?
2. Wo liegen die Daten physisch?
3. Welche Gesetzgebung gilt?
4. Haftung bei Versagen?
5. etc.

Härtung

Das ist ein Zustand einer Komponente, bei dem diese nur noch tut, was sie soll.

1. Überflüssige Software ist deinstalliert.
2. Unbenutzte Kommunikationsprotokolle und Dienste sind abgeschaltet.
3. Offene Kommunikationsschnittstellen sind abgeschaltet oder Heißkleber rein.

Intrusion Detection

Das ist eine automatisierte Überwachungsfunktion.

1. Gegenstand der Überwachung sind alle sicherheitsrelevanten Funktionen eines Systems. Hierunter fallen mindestens
 - a. alle Kommunikationsschnittstellen,
 - b. die Kommunikationsprotokolle,
 - c. die Gesamtheit der ausgeführten Software,
 - d. die Gesamtheit aller im Netzwerk vorhandenen Komponenten und
 - e. alle angemeldeten Benutzer.
2. Ziel der Überwachung ist die Alarmierung beim Eintreten sicherheitsreduzierender Zustände. Hierunter fallen mindestens
 - a. eingesteckte USB-Sticks,
 - b. Anmeldeversuche von Benutzern (gleichzeitige Mehrfachanmeldung, wiederholte Anmeldeversuche, Passwortausprobieren etc.),
 - c. gestartete Software (insbesondere Installer),
 - d. ungewöhnlicher Festplattenzugriff,
 - e. Netzwerk-Scans,
 - f. nicht autorisierte Kommunikationsprotokolle und
 - g. Abweichungen der Benutzungsmuster.

IPsec

Internet Protocol Security ist eine Sammlung von Verschlüsselungsfunktionen. Diese erlauben den Aufbau eines permanenten, verschlüsselten Tunnels durch den alle IP-basierten Protokolle kommuniziert werden können.

IPsec ist Bestandteil des Betriebssystems und wird in unseren Anwendungen zum Aufbau eines VPN (siehe dort) verwendet.

IPsec im TCP/IP-Protokollstapel:

Anwendung	HTTP	IMAP	SMTP	DNS	...
Transport	TCP			UDP	
Internet	IPsec				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

ISMS / Kundenanforderung

Ein Informations-**Sicherheits-Management-System** ist ein Geschäftsprozess, den 99% unserer Kunden etablieren müssen. Im Einzelnen müssen unsere Kunden

1. ein **Inventar** ihrer wichtigsten Informationen aufstellen. Geräteeinstellungen, Datenmodelle und Betriebsdaten fallen hierunter.
Also können wir einen Auszug aus unserer Projektdatenbank liefern.
2. die **Angriffsrisiken** kennen, denen unsere Geräte ausgesetzt sind.
Also können wir ihnen eine Dokumentation der Sicherheitsfunktionen in unseren Geräten liefern. Hierzu gehören Schnittstellen, Kommunikationsprotokolle, Verschlüsselung, Passworte, Sicherheitsmeldungen und Schwachstellenbenachrichtigungen.
3. eine **Risikobewertung** durchführen, um die schlimmsten Risiken zu identifizieren.
Hierbei können wir mit gemeinsamer Diskussions oder einem Bericht zur IT-Sicherheit in einer Anlage helfen. Die Risikobewertung liegt aber schlussendlich beim Betreiber und kann nicht an einen Lieferanten delegiert werden.
4. **Sicherungsmaßnahmen** gegen die schlimmsten Risiken durchführen. Hierfür können wir
 1. Workshops zur IT-Sicherheit geben.
 2. Software-Updates einbringen.
 3. Anlagen umbauen (z.B. alte PCs tauschen.)

Der grundlegende Zweck eines ISMS ist die Risiken für die wichtigsten Unternehmensinformationen zu

1. kennen und zu
2. managen.

„Managen“ bedeutet in diesem Zusammenhang, die Risiken

1. durch **Gegenmaßnahmen** (Korrektur oder Workaround) zu reduzieren,
2. durch **Verzicht** auf eine Funktion zu entfernen,
3. aufgrund von Geringfügigkeit zu **akzeptieren**, oder
4. durch Kauf einer Versicherung auf andere zu **verlagern**.

Kritische Infrastruktur

Eine kritische Infrastruktur ist eine Anlage, deren ungestörter Betrieb im Interesse Deutschlands liegt. Hierunter fallen die Anlagen von 99% unserer Kunden.

Die exakte Definition besteht aus den folgenden zwei Bedingungen.

1. Die Anlage gehört zu den Industriesektoren
 - a. Energie
 - b. Telekommunikation und IT
 - c. Transport
 - d. Gesundheit
 - e. Wasser
 - f. Ernährung
 - g. Finanzen
2. Die Anlage ist groß. (Die hierfür definierten Schwellenwerte finden sich in der Verordnung für kritische Infrastrukturen.)

PKI

Eine **Private Key Infrastructure** ist ein Mittel zur Handhabung von Zertifikaten (siehe Zertifikate und Zertifikatemanagement).

(Wir haben das Thema noch nicht ganz verstanden und heben uns die Fertigstellung für später auf.)

Protokolle - Anwendungsebene

FTP/SFTP/FTPS

Das **File Transfer Protocol** ist ein Kommunikationsprotokoll zur Übertragung von Dateien über IP-Netzwerke.

1. Anwendungsfälle für uns sind das Laden von Datenmodellen oder die Übersendung einer neuen Software-Version auf eine Baustelle.
2. FTP gilt inzwischen als nur noch bedingt einsetzbar, da Benutzername und Passwort unverschlüsselt über das Netzwerk übertragen werden und durch Mithören leicht kompromitiert werden können.

Das **SSH File Transfer Protocol** überträgt Benutzernamen, Passworte und Nutzdaten verschlüsselt.

1. SSH (siehe dort) läuft als separate Software und bewirkt die Verschlüsselung
2. Der FTP-Server selber kommuniziert unverschlüsselt
3. Das benutzen wir zum Zugriff auf P30 und S30.

Das **File Transfer Protocol** über **SSL** überträgt Benutzernamen, Passworte und Nutzdaten verschlüsselt.

1. Die Netzwerkverbindung zum Server ist unverschlüsselt.
2. Die Verschlüsselung erfolgt durch den FTP-Server.

HTTP/HTTPS

Das **HyperText Transfer Protocol** überträgt Webseiten und Benutzereingaben unverschlüsselt.

Das **HyperText Transfer Protocol Secure** überträgt Webseiten und Benutzereingaben (bedenke Passwordeingabe!) verschlüsselt.

Radius

Remote Authentication Dial-In User Service ist ein Kommunikationsprotokoll, [das im Zusammenhang mit Authentifizierung/Authorisierung \(siehe dort\) verwendet wird.](#)

(Wir haben das Thema noch nicht ganz verstanden und heben uns die Fertigstellung für später auf.)

Protokolle - Netzwerkebene

DHP

Text steht aus

HSR

Text steht aus

MRP

Text steht aus

PRP

Text steht aus

RSTP

Das **Rapid Spanning Tree Protocol** wird von Ethernet-Switches ausgeführt. Es Legt fest, auf welchem Weg im Normalbetrieb die Kommunikation läuft und ist im Fall einer Störung zuständig für die Umschaltung auf einen Alternativpfad.

RSTP Enhanced

Text steht aus

SHP

Text steht aus

RBAC

Role Based Access Control (Rollenbasierte Zugriffskontrolle) ist ein Verfahren der zentralen Überwachung und Steuerung von Zugriffen auf Dateien und Dienste durch Personen (und bald auch zwischen Geräten).

Die folgenden Objekte werden zueinander in Beziehung gesetzt:

1. Benutzer – heute eher eine natürliche Person mit Namen und Passwort (und vielleicht weiteren Mitteln der Identifikation... Daumen, Ausweiskarte etc.)
2. Recht – Erlaubnis, eine Aktion (keine zusammengesetzte Transaktion, sondern nur ganz klein) durchzuführen. Beispiel: Schalthandlung auf einem individuellen Trenner.
3. Rolle – ein logischer Behälter für Rechte. Da Rechte zu feinkörnig für eine sinnvolle Vergabe sind, werden sie zusammengefasst. Beispiel: Schaltberechtigter (beinhaltet das Recht zur Schalthandlung auf allen Trennern und Alarmquittierung).

SAM

Der **Substation Administration Manager** ist unser Syslog-Server, der

1. als Senke für Sicherheitsmeldungen (siehe dort) aller Endgeräte im Netz dient,
2. diese Sicherheitsmeldungen einem Sicherheits-Administrator anzeigt und
3. als Informationsquelle für ein Intrusion Detection Systems (siehe dort) dient.

In zukünftigen Versionen soll SAM imstande sein, Authentisierungsanfragen von einem Steuergerät an ein Active Directory (siehe dort) aus einem Stationsnetz hinauszukommunizieren und die Antwort an das Steuergerät zu übermitteln.

Sicherheitsmeldung

Das ist ein sicherheitsbezogenes Meldevolumen in einem Gerät. Dieses Meldevolumen wird von den Betriebsmeldungen unterschieden und richtet sich nicht an Betriebs- sondern Sicherheitspersonal. Unsere Geräte verwenden zur Übertragung das Syslog-Protokoll.

Beispiele für Sicherheitsmeldungen aus P30:

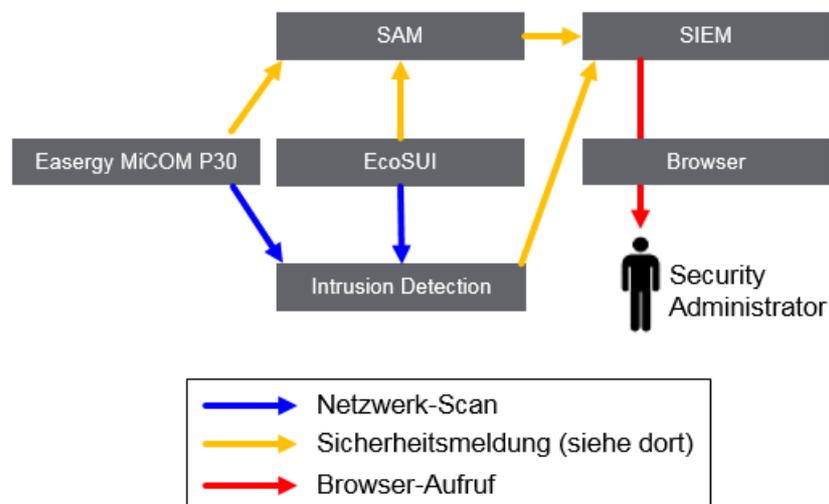
CONNECTION_FAILURE	A connection between the device and a user was not established by the device. The credentials provided by the user were wrong.
CONNECTION_FAILURE_AND_BLOCK	A connection between the device and a user was not established by the device. The credentials provided by the user were wrong. The maximum number of attempts was exceeded, therefore the user was blocked. Unblocking happens either through the security administrator using SAT, or once a configured amount of time has elapsed.
CONNECTION_SUCCESS	A connection between the device and a user has been established. The provided user credentials were ok.
DISCONNECTION	A connection between the device and a user was manually terminated by the user.

SIEM

Ein **S**ecurity **I**nformation and **E**vent **M**anager ist ein Typ Software, der

1. in umfangreichen Listen (siehe SAM) von Sicherheitsmeldungen (siehe dort) nach Mustern sucht,
2. auf vergangene oder laufende Angriffe schließt (siehe Brute Force),
3. die Sicherheitslage eines Systems in einem Dashboard visualisiert und
4. Alarme erzeugt.

Beispiel: jemand versucht sich gleichzeitig in zwei unterschiedlichen Anlagen anzumelden.



SNMP

Das **Simple Network Management Protocol** wird ganz allgemein von einer Netzwerkkomponente (ursprünglich nur Switches) verwendet um Meldungen über ihren Zustand zu versenden.

SSL

Secure Socket Layer ist der Vorgänger von TLS (siehe dort).

Standards

Eine kleine Zusammenstellung von Normen zur IT-Sicherheit.

1. IEC 270xx – Normenreihe zum Management von Risiken der IT-Sicherheit
 1. IEC 27001 – definiert den kreisläufigen Management-Prozess (Investition – Inventar – Risikoerkennung – Risikobewertung – Sicherungsmaßnahmen – Reporting).
 2. IEC 27002 – definiert Sicherungsmaßnahmen.
 3. IEC 27019 – definiert Sicherungsmaßnahmen mit Fokus auf die Energieversorgung.
2. IEC 62351 – beschreibt Verfahren der sicheren Kommunikation. Noch nicht untersucht/verstanden.
3. IEC 62443-x-xx – Normenreihe, die sich an Lieferanten industrieller Automatisierungssysteme richtet.
 1. IEC 62443-1-1 – Terminologie.
 2. IEC 62443-2-1 – Risikomanagement (siehe auch IEC 27001).
 3. IEC 62443-2-3 – Patch Management.
 4. IEC 62443-2-4 – beschreibt einen sicheren Prozess der Leistungserstellung und Lieferung.
 5. IEC 62443-3-3 – Sicherungsmaßnahmen und Sicherheitslevels.
4. IEEE 1686 – noch nicht untersucht/verstanden.
5. IEEE C37.240 – noch nicht untersucht/verstanden.
6. NERC CIP – das **Northamerican Electric Reliability Corporation Critical Infrastructure Protection** ist ein US/Kanada-Gesetz mit internationaler Verbreitung, das Sicherheitsanforderungen gegen Produkte und Organisationen enthält. Hier kennt und will das keiner, weil wir die ISMS (siehe dort) gemäß IEC 27000 (siehe dort) bevorzugen. - Bislang haben wir keinen Inhaltsvergleich gemacht.
7. NIST 800 – noch nicht untersucht/verstanden.
8. WIB 2.0 – das ist ein Vorläufer der IEC 62443-2-4.

Anforderungen der Art "Die folgenden Standards müssen eingehalten werden..."

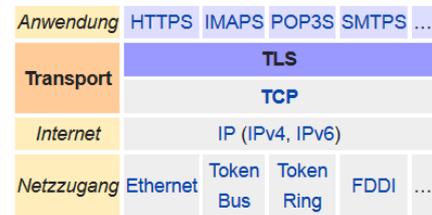
1. sind von technischen Normen inspiriert (Ein Auto darf maximal 2,5m breit sein!),
2. entsprechen nicht dem Sinn eines ISMS (siehe dort) und
3. sollten wir mit einem Besuch/Gespräch beantworten.

TLS

Transport Layer Security ist ein Ver- und Entschlüsselungsmechanismus.

Implementierungen findet man in Betriebssystemen. Man kann sie aber auch als externes Produkt kaufen und im eigenen Produkt zum Einsatz bringen.

TLS im TCP/IP-Protokollstapel



Das eigene Produkt kommuniziert dann „durch“ das TLS mit der Außenwelt. Auf der Gegenseite muss dann die eingehende, verschlüsselte Kommunikation durch eine TLS-Funktion derselben Version wieder entschlüsselt werden.

Die Versionen <= 1.2 gelten gemeinhin als gehackt, weswegen wir als Hersteller Anlass haben, unsere alten Implementierungen auszutauschen.

Hier die TLS-Implementierungen in unseren Produkten (Stand Mai 2018).

Ethernet and Application Protocols			
Product	Protocol	Communication Partner	Encryption
CAT	DPWS	C264	TLS 1.0
ClearSCADA	HTTPS	web browsers	TLS 1.1
ClearSCADA	HTTPS	web browsers	TLS 1.2
ClearSCADA	OPC XML DA	PLCs	TLS 1.0
ClearSCADA	OPC XML DA	Master station	TLS 1.0
Easergy MiCOM P30/C434	DPWS	SAT	TLS 1.0
Easergy MiCOM P30/C434	SecureCom	Easergy Studio	TLS 1.0
Easergy MiCOM P40	DPWS	SAT	TLS 1.0
Easergy MiCOM P40	SecureCom	Easergy Studio	TLS 1.0
Easergy Studio	SecureCom	P30, P40, C434	TLS 1.0
EcoSUI	DPWS	SAT	TLS 1.0
GAT	DPWS	PACiS Gateway	TLS 1.0
MiCOM C264	DPWS	SAT	TLS 1.0
MiCOM S30	HTTPS	web browsers	TLS 1.0
PACiS Gateway	DPWS	SAT	TLS 1.0
Saitel DR	DPWS	SAT	TLS 1.0
SAM	HTTPS	web browsers	TLS 1.0
SAT	DPWS	IEDs with DPWS servers, su	TLS 1.0
SAT	DPWS	SAM	TLS 1.0

(Siehe auch VPN.)

Upgrade / Update

Ein *Upgrade* ist eine Funktionserweiterung und gehört zur strategischen Produktentwicklung (etwa Windows 7 auf Windows 10).

Ein *Update* ist eine Korrektur an Software oder Geräteeinstellungen. Updates werden nötig bei

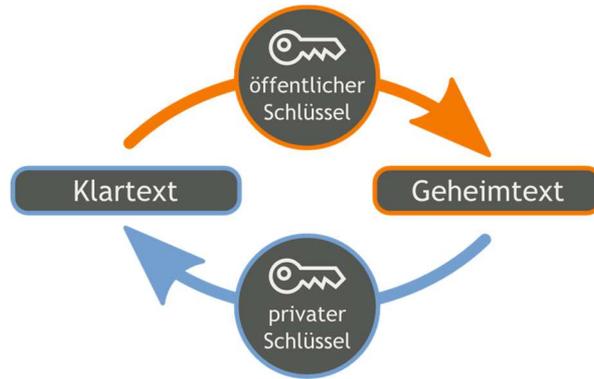
1. Produktmängeln (Vertragsabweichungen).
2. Bugs (Nichterfüllung einer Anforderung).
3. Schwachstellen (Reduzierung der IT-Sicherheit).

Verschlüsselung

Verschlüsselung ist eine Maßnahme zur Unkenntlichmachung von Informationen.

Entschlüsselung ist eine Maßnahme zur Wiederkenntlichmachung verschlüsselter Informationen.

Asymmetrische Verschlüsselung entspricht dem folgenden Bild.



VPN

Ein **Virtual Private Network** definiert eine exklusive Gruppe von Kommunikationspartnern, die verschlüsselt über das Internet kommunizieren.

VPNs gibt es grundsätzlich in zwei Ausprägungen:

1. SSL/TLS (siehe dort) – Verwendung für temporäre Verbindungen, etwa auf mobilen Endgeräten.
2. IPSec (siehe dort) – Verwendung für dauerhafte Verbindungen, etwa Pulse/Homeoffice oder Fernzugriff auf Kundenanlagen.

VLAN

Ein **Virtual Local Area Network** ist

1. ein Mittel zur Trennung und Priorisierung von Datenübertragungen
2. in einem gemeinsamen, physischen Netzwerk.

So kann etwa sichergestellt werden, dass die Übertragung von Wartungsinformationen (remote Desktop, Datenmodell Laden) keinen negativen Einfluss auf die Betriebskommunikation (Statusmeldungen, Befehle) hat.

Die VLAN-Funktion wird auf den folgenden Ebenen implementiert.

1. Geräteebene – auf einer physischen Kommunikationsschnittstelle werden zwei Informationstypen unter unterschiedlichen IP-Adressen gemeldet.
2. Switches – die IP-Adressenkreise für Wartung und Betrieb sind hier bekannt und erlauben die getrennte Weiterleitung der Telegramme an die Zieladressen.

Die Clients (HMI, Einstelltools) sind Empfänger der Information und benötigen keine VLAN-Implementierung.

Zertifikat

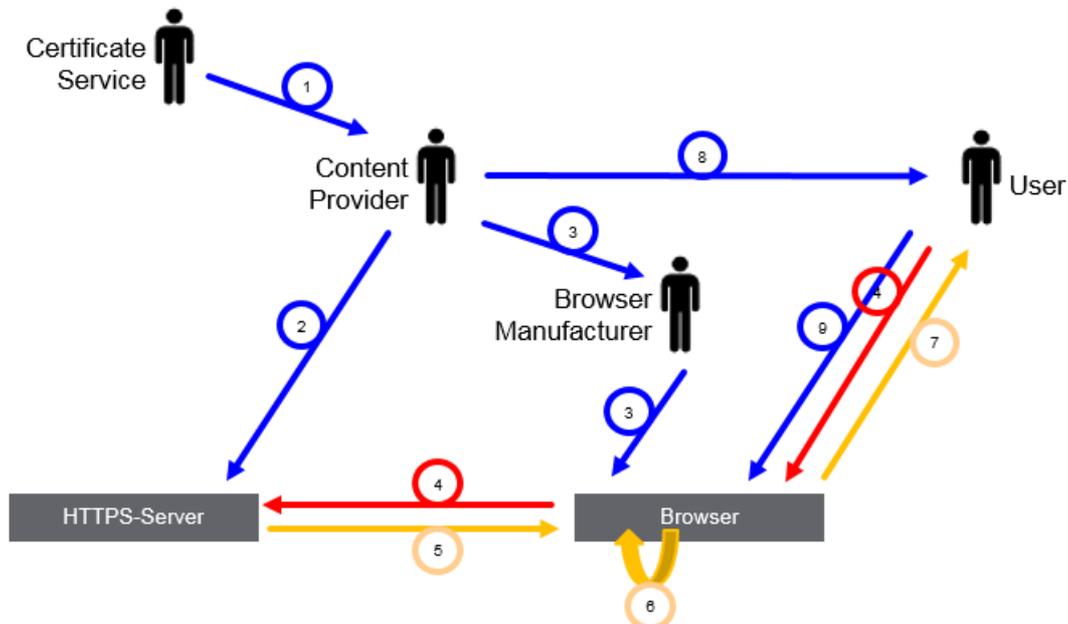
Das ist eine Datei. Ihr

1. Inhalt und der
2. Prozess ihrer Verwendung

erlauben einen sicheren Rückschluss auf den Urheber einer Information.

Beispiel: „Wie kann ich sicher wissen, dass mein Nachrichtenaufwurf tatsächlich von www.tagesschau.de und nicht (siehe Angriffsmethode Man-in-the-Middle) von jemand anderem beantwortet wurde?

Im Folgenden eine Illustration. (Völlig klar, dass das heftig ist. Die animierte PPT-Version kann bei uns abgerufen werden.)



1. Das Zertifikat wird erzeugt und an den Webseitenbetreiber geliefert.
2. Der Webseitenbetreiber platziert das Zertifikat auf seinem Webserver.
3. Der Webseitenbetreiber übergibt das Zertifikat einem Browser-Hersteller, der es standardmäßig mit seinem Produkt liefert.
4. Ein Benutzer verwendet den Browser und ruft eine Webseite auf.
5. Der Webserver liefert die Antwort und schickt das Zertifikat mit.
6. Der Browser stellt die Gleichheit zwischen dem erhaltenen und dem bereits installierten Zertifikat fest und beweist damit die Identität vom Webserver.
7. Der Browser zeigt die angeforderte Webseite dem Benutzer an.
8. Der Betreiber des Webservers macht das Zertifikat verfügbar, sodass...
9. ... Benutzer es eigenständig in ihrem Browser installieren können.

Zertifikatsmanagement

Eine zusammenfassende Bezeichnung der folgenden Prozesse.

1. Erstellung
2. Lieferung
3. Weitergabe
4. Installation
5. Authentifizierung
6. Gültigkeitsdauer
7. Sperrung
8. Entwertung/Rücknahme

Uns betrifft das praktisch im Zusammenhang mit

1. Verschlüsselter Kommunikation
 - a. E-Mails
 - b. HTTPS

- c. VPN
- 2. Signierung von gelieferter Software (können wir aber noch nicht).