Informationssicherheit und Datenschutz im Smart Home

Alexander Matheus
13. Juli 2021

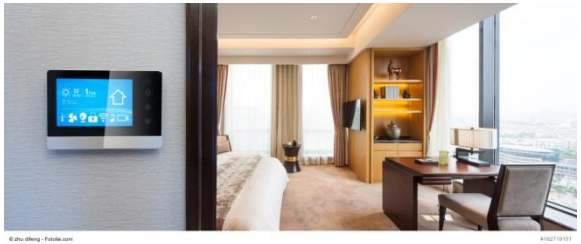
VDE INSTITUT

VDE Prüf- und Zertifizierungsinstitut

- Gegründet 1920 und weltweit tätig
- Mehr als 100.000 Prüfungen jährlich
- Der Bereich „Smarte Technologien“ wurde 2012 gegründet:
  - Informationssicherheit
  - Funktionale Sicherheit

- Informationssicherheitsprüfungen an Smart Home Systemen, IoT-Systemen, Medizintechnik, Industrie 4.0 Systemen
- Konformitätstests und Penetrationstests im eigenen Labor

Informationssicherheit / Cyber Security ist ein Querschnittsthema



Smart Home

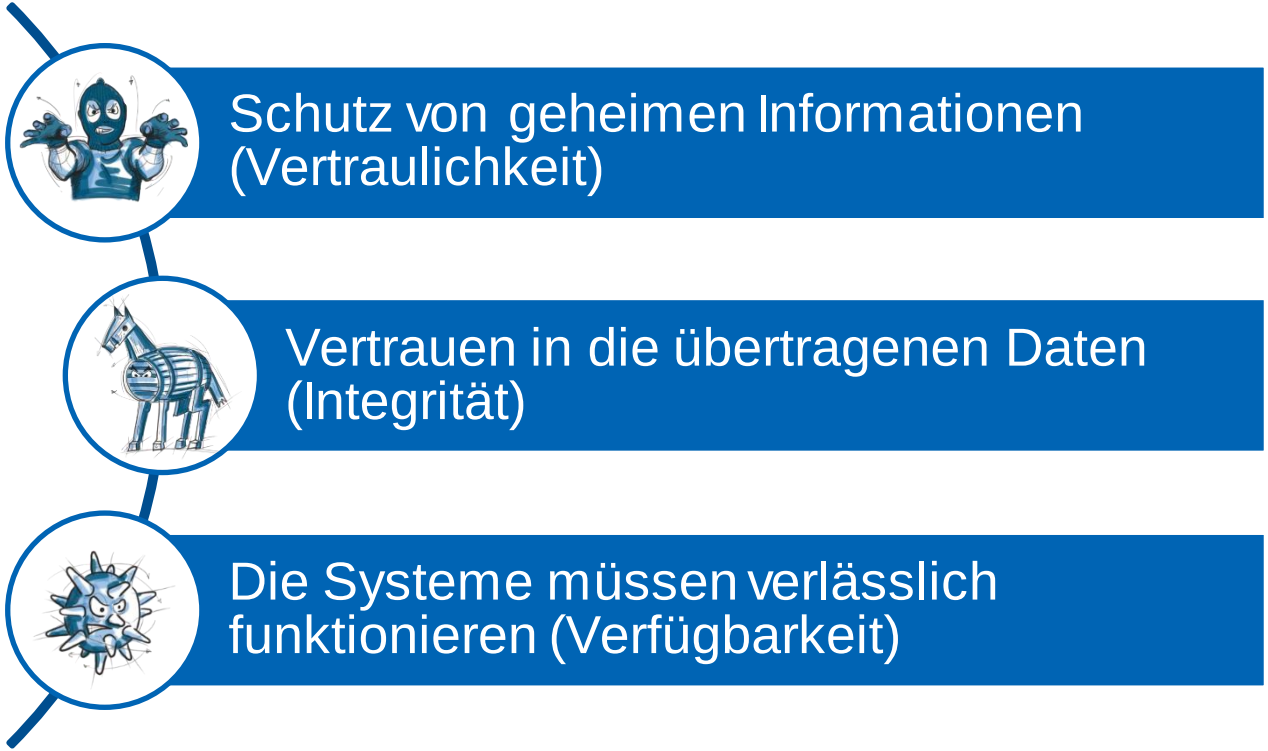
Medizintechnik

IoT (Internet of things)/Vernetzte Haushaltsgeräte

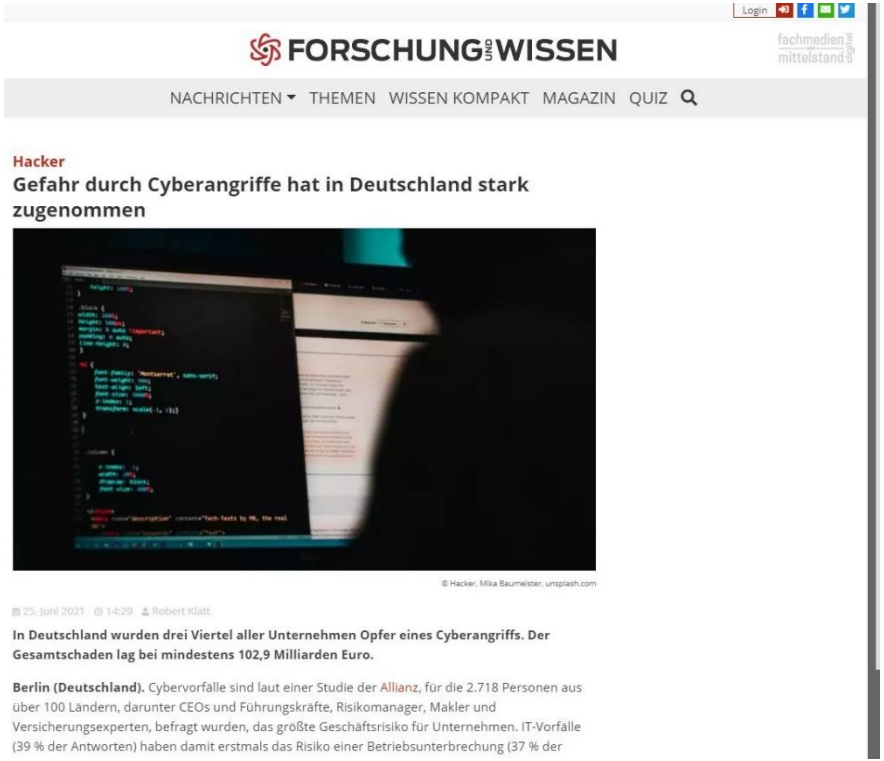
Automotive

Industrie 4.0

Herausforderungen für Hersteller und Betreiber



Bedrohungen



Login

FORSCHUNG UND WISSEN

fachmedien mittelstand

NACHRICHTEN THEMEN WISSEN KOMPAKT MAGAZIN QUIZ

Hacker

Gefahr durch Cyberangriffe hat in Deutschland stark zugenommen

© Hacker, Mika Baumeister, unsplash.com

25. Juni 2021 14:29 Robert Klatt

In Deutschland wurden drei Viertel aller Unternehmen Opfer eines Cyberangriffs. Der Gesamtschaden lag bei mindestens 102,9 Milliarden Euro.

Berlin (Deutschland). Cybervorfälle sind laut einer Studie der Allianz, für die 2.718 Personen aus über 100 Ländern, darunter CEOs und Führungskräfte, Risikomanager, Makler und Versicherungsexperten, befragt wurden, das größte Geschäftsrisiko für Unternehmen. IT-Vorfälle (39 % der Antworten) haben damit erstmals das Risiko einer Betriebsunterbrechung (37 % der

- Einfalltor für Trojaner
- Auslesen persönlicher Daten
- Überwachung
- Stalking/Terrorisieren
- Deaktivieren von Geräten
- Missbrauch von Ressourcen
  - Bot-Netz (DDOS)
  - Cryptomining/Cryptojacking

Übersicht der Regulierungsaktivitäten

Gesetzlich vorgeschrieben

- IT-Sicherheitsgesetz (2.0): KRITIS - für Kritische Infrastrukturen: u.a. ISO/IEC 27001
- EU-DSGVO (Datenschutzgrundverordnung)

Nationale Anforderungen

- BSI Anforderung an SmartMeter Gateways

Europäische Anforderungen

- Cyber Security Act: “Voluntary EU cybersecurity certification framework for ICT products”
- RED (Radio equipment directive): Kapitel 3.3.e (privacy), 3.3.f (fraud) erhalten zusätzliche Anforderungen durch delegierten Rechtsakt

International

- UK: Resultierende Anforderungen aus Brexit
- USA: FDA Guidance Cyber Security (Medizintechnik), lokale Anforderungen
- China: Cyber Security Law (z.B. EU Befürchtung zur Abschaltung von VPN Tunneln)

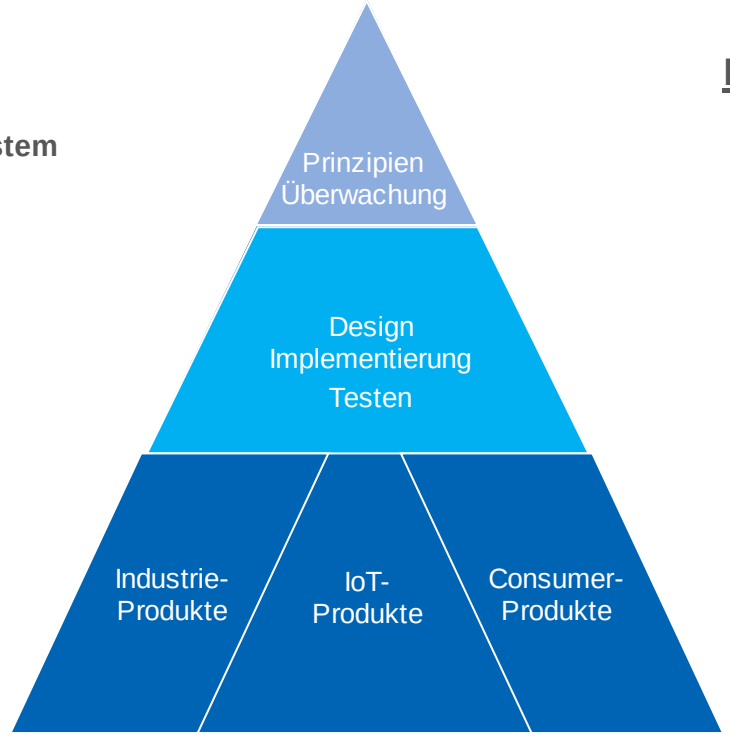
Cyber Security Gesamtbetrachtung - Hersteller

Unternehmensebenen

Cyber Security **Management System**

Cyber Security **Development**

Cyber Security **Product Security**



Normenlandschaft

ISO 27001
IEC 62443-2-1

IEC 62443-4-1
(ETSI 303 645)

IEC 62443-4-2
ETSI 303 645
VDE-PB-0004, VDE-PB-0005

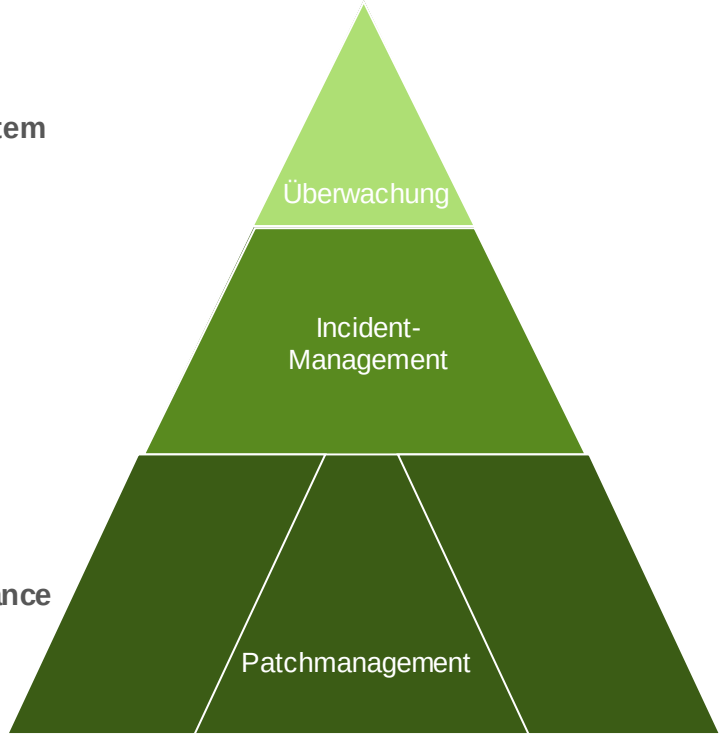
Cyber Security Gesamtbetrachtung - Betreiber

Unternehmensebenen

Cyber Security **Management System**

Cyber Security **Monitoring**

Cyber Security **Product Maintenance**



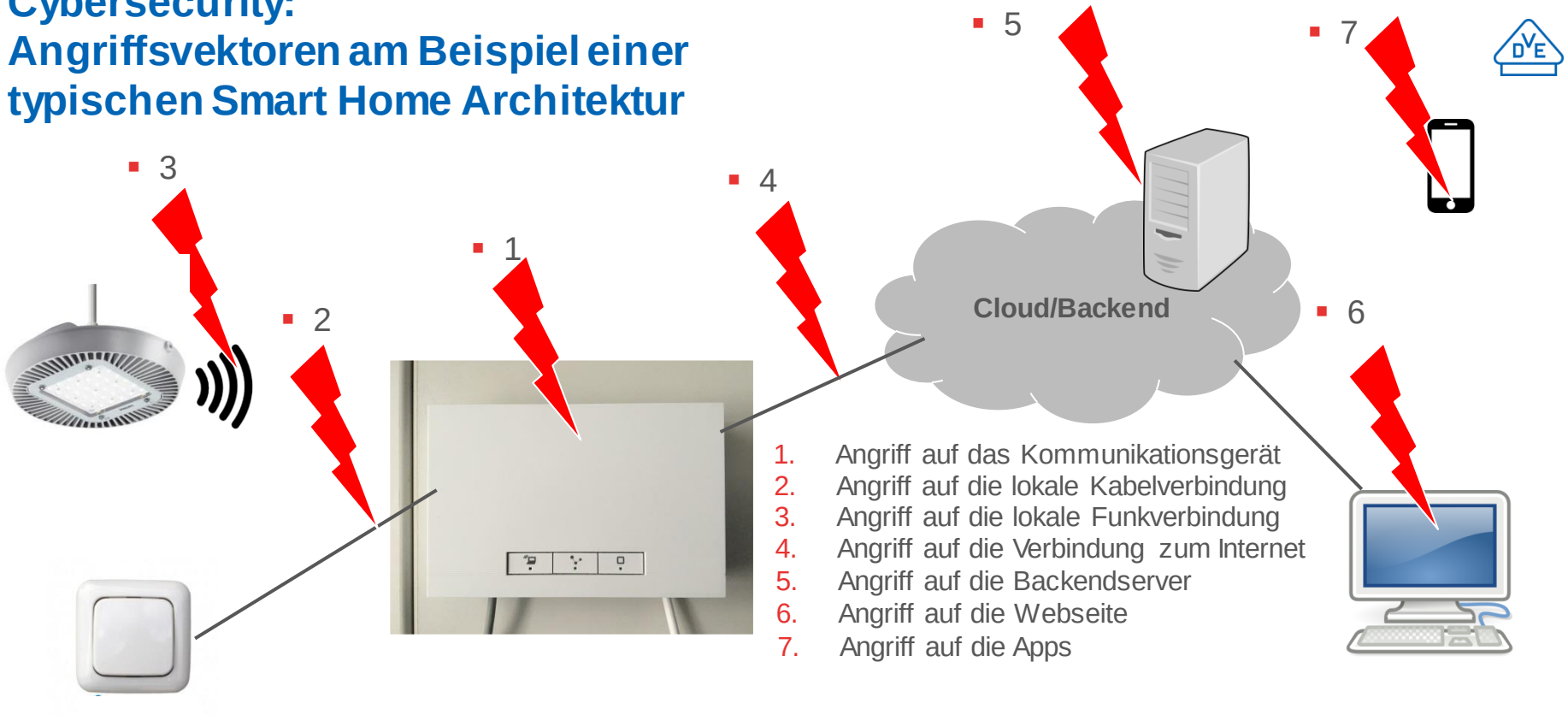
Aufgaben

Risikoüberprüfung

Informationspflichten
Regelmäßige Sicherheitsüberprüfungen
Updates

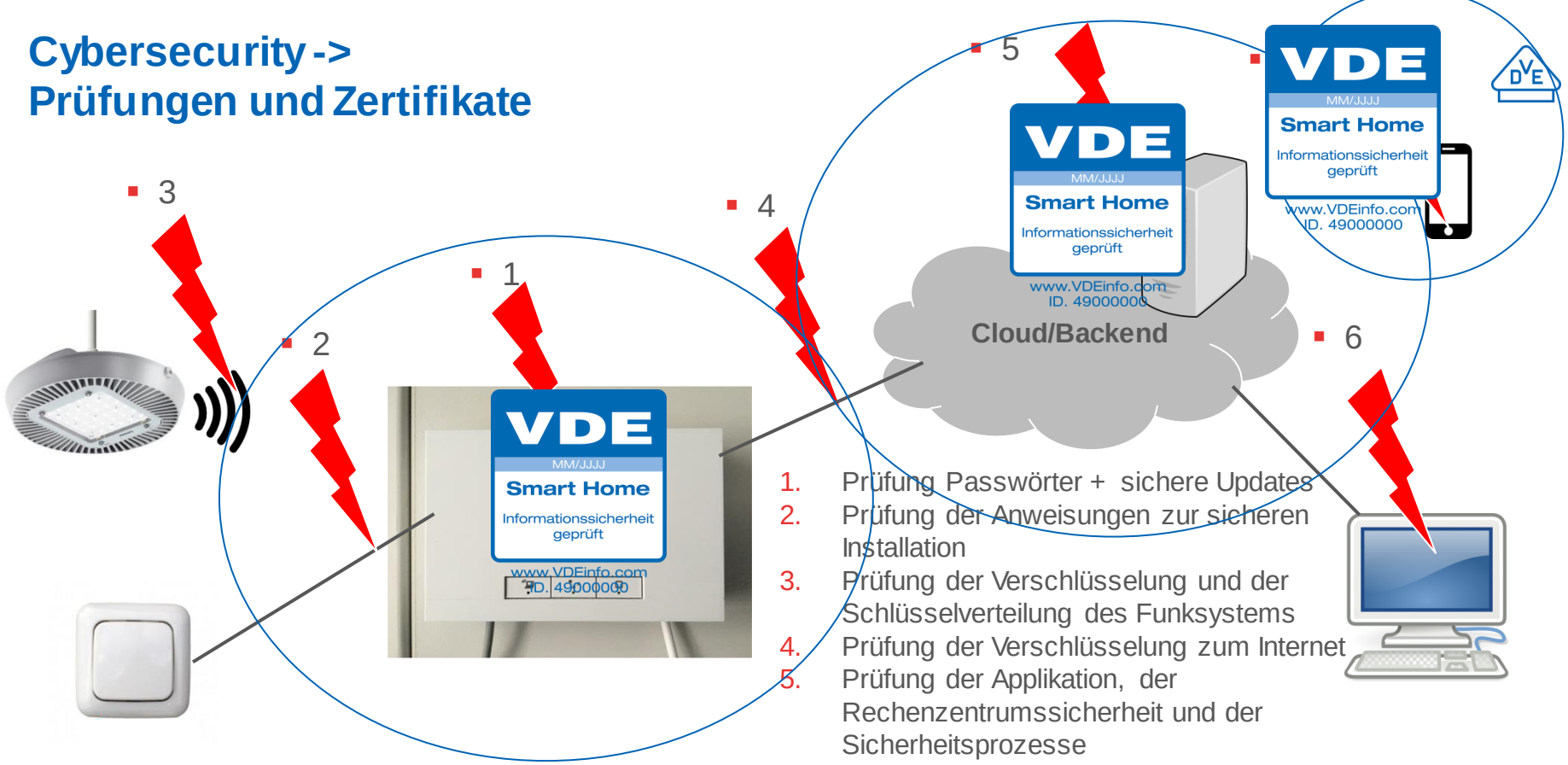
Sicherheitsupdates

Cybersecurity: Angriffsvektoren am Beispiel einer typischen Smart Home Architektur



1. Angriff auf das Kommunikationsgerät
2. Angriff auf die lokale Kabelverbindung
3. Angriff auf die lokale Funkverbindung
4. Angriff auf die Verbindung zum Internet
5. Angriff auf die Backendserver
6. Angriff auf die Webseite
7. Angriff auf die Apps

Cybersecurity ->
Prüfungen und Zertifikate



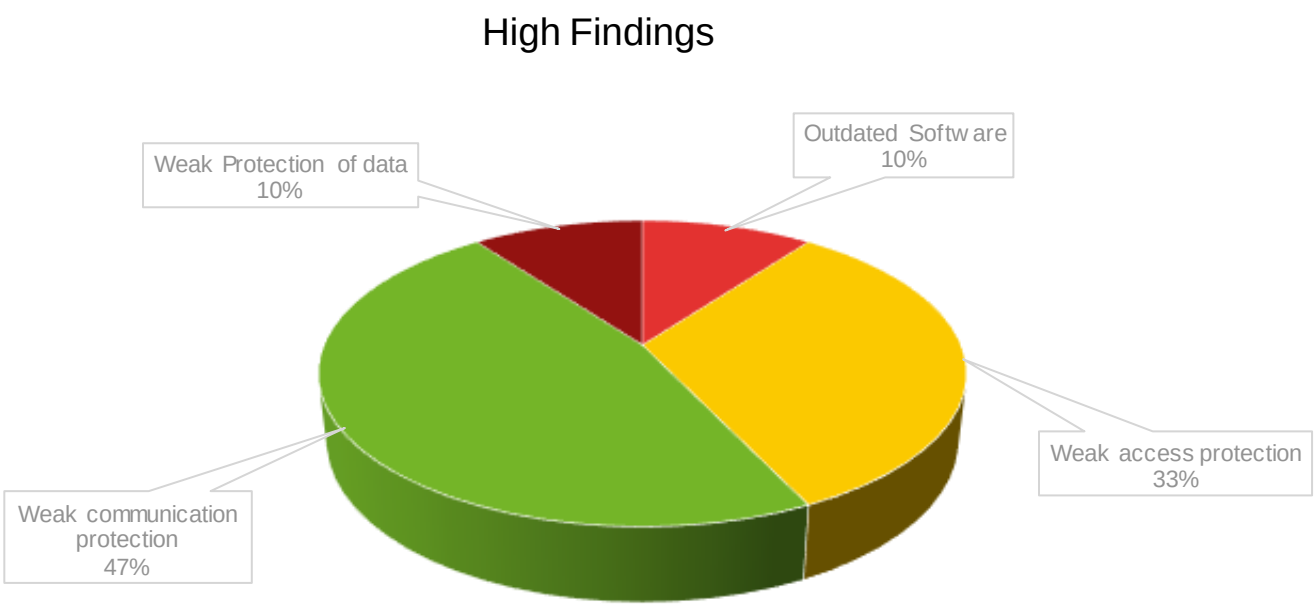
1. Prüfung Passwörter + sichere Updates
2. Prüfung der Anweisungen zur sicheren Installation
3. Prüfung der Verschlüsselung und der Schlüsselverteilung des Funksystems
4. Prüfung der Verschlüsselung zum Internet
5. Prüfung der Applikation, der Rechenzentrumssicherheit und der Sicherheitsprozesse
6. Prüfung der Webanwendung
7. Prüfung der Apps

VDE INSTITUT

IOT: Prüfung der Kommunikationsgeräte, Cloud + Apps

- **Prüfung der IOT Systeme:**
  - Kommunikationsgeräte (z.B. Gateways)
  - Backend/Cloud Systeme
  - Apps
- **Sicherheitsziele**
  Werden alle geforderten Sicherheitsziele erfüllt?
- **Penetrationstest**
  Ist die Implementierung wirksam?
- **Lebenszyklus Prüfung**
  Wird die Informationssicherheit in allen Phasen des Lebenszyklus von der Installation über die Wartung bis zur Stilllegung gewahrt?

Ergebnisse bei Cybersecurity Prüfungen



Final draft ETSI EN 303 645 V2.1.1 (2020-06) (European institute for Telecommunication)

CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

- Produkteigenschaften
- Kryptografische Anforderungen
- Prozess Anforderungen
- Anforderungen an den Datenschutz

Projekt Durchführung ETSI EN 303 645

1. Dokumente:

- Product document check and cross-check with table B1 (Gap-analysis)
- Process document check (Gap-analysis)

2. Produkt Tests:

- Product feature tests
- Produkt pentests
  including partial source code analysis

Conformity Checklist - TL43 0240 A3 - ETSI EN 303 645 V2.1.1 (2020-06)

clause	Requirement	Mandatory/ Recommendation	Condition fulfilled	Requirement Summary*	Test Type	Specific Pentest	Pass/Fail Criteria
5.3-14	Provision 5.3-14 R C (3, 4)	R		For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.	Document		The information for the support and replacement must be available for the user.
5.3-15	Provision 5.3-15 R C (3, 4)	R		For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.	Document		The information for the isolation and replacement must be available for the user.
5.3-16	Provision 5.3-16 M	M		The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.	Document Feature Test		The IoT device must be recognizable.
	5.4 Securely store sensitive security parameters						
5.4-1	Provision 5.4-1 M	M		Sensitive security parameters in persistent storage shall be stored securely by the device.	Document Pentest	Vulnerability test	The storage must be performed in a secure way.
5.4-2	Provision 5.4-2 M C (10)	M C		Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.	Document Pentest	Vulnerability test	Tampering resistance must be implemented.
5.4-3	Provision 5.4-3 M	M		Hard-coded critical security parameters in device software source code shall not be used.	Document Pentest	Source code inspection	The source code inspection must not identify any security parameters.
5.4-4	Provision 5.4-4 M	M		Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with	Document Pentest	Vulnerability test	The security parameters must be unique per device.

Neue Prüfbestimmung VDE-PB-0030

- VDE geprüfte Datensparsamkeit

  https://www.vde.com/tic-de/news/2021/privacy-by-design-privacy-by-default
  -> Informationen auf der VDE Webseite

- Zweiteilige Prüfung
  1. Dokumentenprüfung -> Privacy-by-design
  2. Implementierungsprüfung -> Privacy-by-default

  - Ziel ist es, die Datensparsamkeit des Systems nachzuweisen

Datenschutz: Neue Prüfbestimmung VDE-PB-0030

1. Noch keine Zertifizierungsmöglichkeit gemäß EU-DSGVO in naher Zukunft in Sicht. Akkreditierungsprozess bei der DAkkS kann gestartet, aber noch nicht abgeschlossen werden. Technische und juristische Experten werden benötigt.
2. Nachweis der Datensparsamkeit nach den Prinzipien „Privacy-by-design“ und „Privacy-by-default“ möglich und zertifizierbar

Cybersecurity

Informationen haben einen hohen Wert für Unternehmen, Behörden sowie Privatpersonen und müssen daher angemessen geschützt werden. Ein vertrauenswürdiger Umgang mit diesen Informationen sowie deren Schutz sind die wesentlichen Ziele der Informations-sicherheit.

Erhalten Sie hier und heute wertvolle Tipps, für Ihre Datensicherheit!

Die sieben Regeln der Informationssicherheit:

1. **Sichere Passwörter verwenden!**
   Definieren Sie für jeden Service ein eigenes, starkes Passwort.

2. **Verfügbare Sicherheitseinstellungen verwenden!**
   Nutzen Sie beispielsweise die Zwei-Faktoren-Authentifizierung.

3. **Systeme aktuell halten!**
   Führen Sie regelmäßig Updates durch.

4. **Regelmäßig Backups der eigenen Dateien erstellen!**
   Sichern Sie Kopien Ihrer Daten.

5. **Vorsicht beim Öffnen von Dateien oder Links!**
   Klicken Sie nur auf externe Inhalte von vertrauenswürdigen Personen.

6. **Vorsicht bei der Verwendung von externer Hardware!**
   Nutzen Sie nur Ihre eigenen USB-Sticks oder externen Festplatten bzw. solche von vertrauenswürdigen Personen.

7. **Auf externe Prüfungen der Informationssicherheit achten!**
   VDE-Zertifikate bieten Ihnen einen Hinweis darauf, dass Ihre Daten geschützt sind.

VDE INSTITUT

VDE INSTITUT

Zusammenfassung

1. Alle Systeme und Produkte, die Daten austauschen (z.B. über Apps), sind angreifbar und werden auch aktiv angegriffen.
2. Zur Zeit gibt es wenige Anforderungen und Vorgaben für Produktentwickler – Änderungen dazu zeichnen sich aber ab.
3. Die ETSI EN 303 645, die Basisanforderungen für IOT Systeme aufzeigt, wird an Bedeutung gewinnen.
4. Das VDE Prüf- und Zertifizierungsinstitut bietet produktübergreifende Services an, um Produkte sicherer zu machen und die Sichtbarkeit nach außen zu erreichen.

www.VDEinfo.com
ID. 49000000

www.VDEinfo.com
ID. 49000000

www.VDEinfo.com
ID. 49000000

www.VDEinfo.com
ID. 49000000

www.VDEinfo.com

www.VDEinfo.com
ID. 49000000

VDE INSTITUT

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Alexander Matheus
Senior Expert
Informationssicherheit
Tel. +49 69 8306-499
alexander.matheus@vde.com

VDE INSTITUT