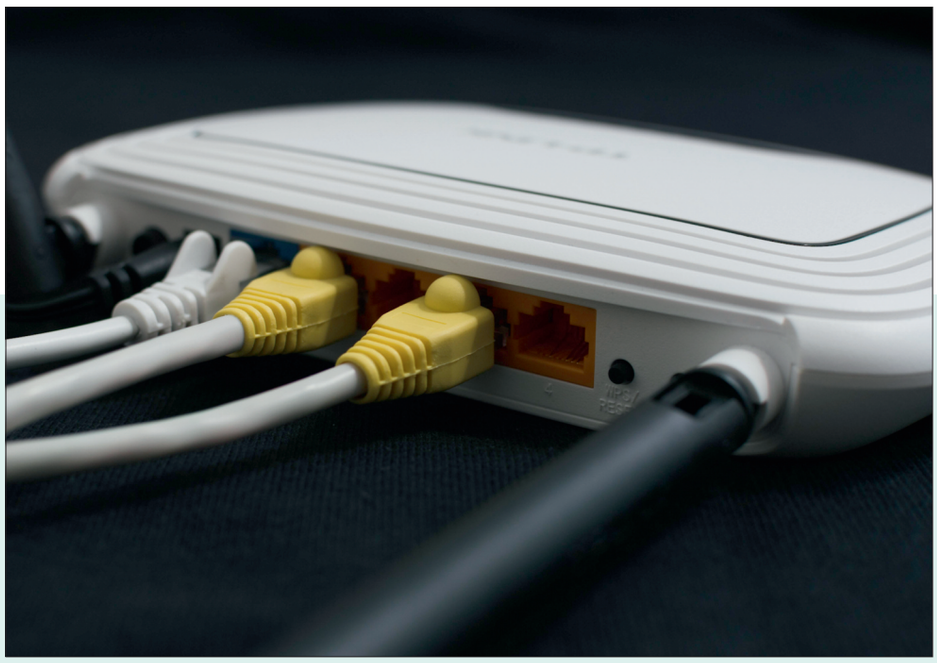
Erste VdS-Zertifizierung für Cyber-Sicherheit bei Übertragungsgeräten

Funktionale IT-Sicherheit dank VdS 3836 – den Hackern ein Schnippchen schlagen



Durch die ständige Verbindung mit dem Internet müssen auch Gefahrenmeldeanlagen angemessen geschützt sein (Foto: Lorenzo Cafaro via Pixabay)

Dass das Internet kein sicherer Ort ist, weiß inzwischen auch jeder Laie. Das ganze Ausmaß der Bedrohungen wird jedoch auch von Experten gerne verdrängt. Tagtäglich steigt die Zahl der bekannten Sicherheitslücken und dementsprechend auch die der Schadsoftwares, die diese Lücken ausnutzen können. Althergebrachte Schutzmaßnahmen wie Virenscanner und Firewalls reichen da allein nicht mehr aus, wenn sensible Bereiche geschützt werden sollen. Besonders bei vernetzten Geräten im Bereich des „Internet of Things" (IoT) lässt die Cyber-Sicherheit oft zu wünschen übrig. s+s report sprach mit Daniel Kaumanns von TAS und Sebastian Brose von VdS über dieses aktuelle Thema und über adäquate Lösungen.

s+s report: Fangen wir zunächst ganz grundlegend an: Wie kann man sich einen Hacker-Angriff auf Anlagen und Produkte der Sicherheitstechnik vorstellen? Und welche Folgen kann so ein Angriff haben?

Daniel Kaumanns: Hacker können beispielsweise den Remote-Zugriff auf Anlagen und Produkte nutzen. Dieser Remote-Zugriff wird eingerichtet, damit der Errichter oder der Betreiber aus der Ferne die Anlage, etwa eine Einbruchmeldeanlage, konfigurieren oder warten kann. Dazu muss diese Anlage mit dem Internet verbunden sein, was in der gängigen Praxis leider meist über einen konventionellen Router geschieht. Für einen direkten Fernzugriff werden noch heute einfach Ports im Router selbst freigegeben, über die die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Mit jedem geöffneten Port steigt jedoch das Risiko, angreifbar zu werden. Wenn zudem unsichere Kennwörter verwendet werden und/oder die Software der Endgeräte veraltet ist, haben selbst weniger versierte Cyber-Kriminelle leichtes Spiel beim Zugang zum System.

Sebastian Brose: Nicht nur im Bereich der kritischen Infrastruktur kann dies fatale Folgen haben. Was passiert etwa, wenn eine Einbruchmeldeanlage Alarme nicht mehr übertragen kann? Oder wenn komplette Anlagen stillstehen, weil Kernkomponenten ausfallen? Hier ist die Sicherheit von Menschen, Unternehmenswerten und Gebäuden bedroht!

s+s report: Angesichts dieser Bedrohungslage stellt sich die Frage: Was zeichnet einen sicheren Remote-Zugang aus?

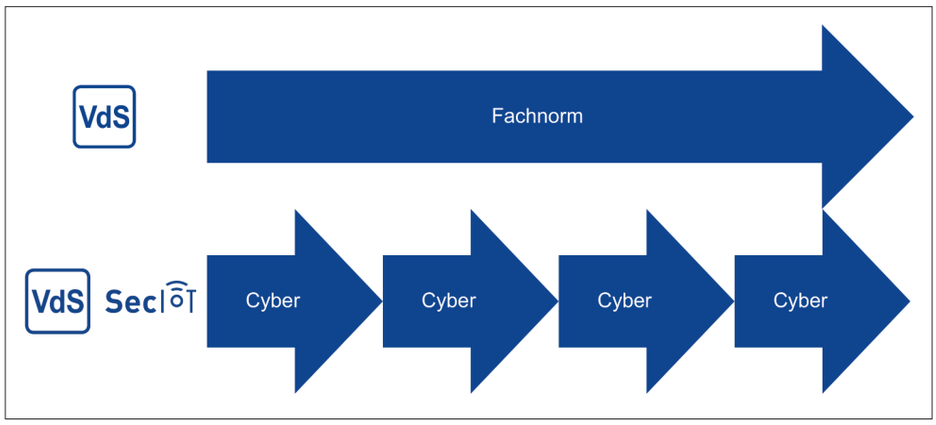
Sebastian Brose: Dass einfach Ports im Router freigegeben werden, sollte ein für alle Mal der Vergangenheit angehören. Stattdessen sollen sichere Konstrukte genutzt werden, beispielsweise mit einem Trust-Anchor, einer Art Vermittlungsstelle oder Plattform im Internet, zu der

sich beide Seiten aktiv verbinden. Neben der Systemarchitektur mit beispielsweise einer sicheren Plattform müssen auch die Komponenten wie die Übertragungseinrichtung optimal geschützt werden.

Die Übertragungseinrichtung ist ja nicht nur für den Fernzugriff immer online, sondern in erster Linie für die Alarmübertragung. Für beides hat das Unternehmen TAS Sicherheits- und Kommunikationstechnik eine VdS-anerkannte Lösung: ein sicheres Gateway für die Übertragung von Alarmen, Sprache und (Monitoring-)Daten sowie eine sichere Infrastruktur für den Remote Access.

s+s report: Herr Kaumanns, welche Übertragungsgeräte Ihrer Firma tragen das VdS-Siegel?

Daniel Kaumanns: Die von TAS entwickelten Übertragungsgeräte TAS-Link IV und SIRO-Port sind die ersten in Deutschland, die nach VdS 3836 zertifiziert sind und somit das SecIoT-Siegel tragen dürfen. Dieses Siegel zeichnet eine besondere Eignung der Cyber-Sicherheit für Komponenten der Brandschutz- und Sicherheitstechnik aus. Durch das proprietäre Betriebssystem können die Zugriffsmöglichkeiten von vornherein auf die Ports beschränkt werden, die auch wirklich benötigt werden. Neben diesem Schutz durch „Security by Design“ unterstützt die neue Generation von TAS-Link- und SIRO-Port-Übertragungsgeräten auch das Protokoll IPsec für die verschlüsselte Datenübertragung und bietet weitere Sicherheitsfeatures, die dem höchsten Level der Cyber-Security entsprechen. Ein unberechtigter Zugriff auf die Übertragungsgeräte ist damit nahezu unmöglich.



Produkte müssen bzgl. Cybersicherheit schnelleren Überarbeitungszyklen folgen (Grafik: VdS)

s+s report: Die zertifizierte Technik ist aber nur ein Baustein für eine sichere Einrichtung des Fernzugriffs. Welche weiteren Komponenten sind wichtig?

Sebastian Brose: Wie vorhin bereits angedeutet: Die gesamte Infrastruktur für den Remote-Zugriff spielt ebenso eine wichtige Rolle. Bereits im letzten Jahr hat die Firma TAS eine VdS-Zertifizierung für die in ihrem Hause entwickelte „TAS Secure Platform“ erhalten. Auch hier war das Unternehmen Vorreiter in puncto Cyber-Sicherheit und der erste Remote Access Infrastructure Service Provider (RAISP), der in Deutschland durch VdS zertifiziert wurde. Erfüllt wurden dabei nicht nur die hohen Sicherheitsanforderungen an die Infrastruktur der Fernzugriffsplattform, sondern auch die Anforderungen an den Service Provider. Dieser ist schließlich verantwortlich für sichere, ständig verfügbare Verbindungen und für den Schutz gegen Cyber-Angriffe.

Zertifikatsübergabe bei der Firma TAS in Mönchengladbach: (v. l. .n. r.) Christoph Schäfer, Produktmanager bei TAS, Günter Grundmann, Abteilungsleiter im VdS-Labor für elektronische Sicherungstechnik, und Daniel Kaumanns, verantwortlicher Produktmanager für die TAS Secure Platform (Foto: VdS)

Bislang fehlte es in der Normenwelt an klaren Regeln für den Fernzugriff auf Alarmsysteme – mit der Folge von Haftungsrisiken für die Betreiber. Mit den kommenden Normen TS 50136-10 für Remote Access und EN 50710 für Remote Services ändert sich zukünftig die unklare Lage.

Daniel Kaumanns: Beide VdS-Zertifizierungen sind ein Gütesiegel für unsere Arbeit an der Cyber-Sicherheit in der Übertragungstechnik. Unser Ziel war es, eine ganzheitlich sichere Lösung für Remote Services anbieten zu können – angefangen bei der Infrastruktur über Gateways bis hin zur Verantwortungsübernahme für den sicheren Fernzugriff auf Gefahrenmeldeanlagen. Kunden, die unsere Plattform sowie flexibel buchbare Services nutzen, bezahlen monatlich nur für die Remote Dienste, die auch benötigt werden. Es muss weder in eine eigene Infrastruktur noch in den Betrieb oder in die Weiterentwicklung investiert werden.

Sebastian Brose: Hier zeigt sich, dass bei Monitoring und Fernwartung von Gefahrenmeldeanlagen

Allgemeine Anforderungen	Benutzer-/ Zugriffsmanagement	Vertraulichkeit und Integrität	Protokollierung/ Ereigniserfassung	Datenfluss	begleitende Maßnahmen
Offline-Funktionalität	Zugriffsschutz durch Authentisierung	Transport-verschlüsselung	Audit Log	sichere Kopplung	Dokumentation der Komponente
sicherer Grundzustand	keine festen Codes	Integrität der Daten bei der Übertragung	Benachrichtigung bei sicherheitsrelevanten Ereignissen	Fremdprodukte/ -dienste	umfassende Bereitstellung von Support
Anpassung der Konfiguration	individualisierte Benutzerkonten	Gewährleistung der Integrität der Software	Export von Ereignissen	„Call-Home"-Funktion	automatische Update-Prüfung
Handhabung von Fehlfunktionen/ Störungen	minimale Zugriffsrechte von Benutzerkonten	Plausibilität von Benutzereingaben/ -aktionen	Erfassung von Telemetriedaten	Verwaltung von Schnittstellen	
Schnittstellen-Sicherheit	zusätzlicher Schutz kritischer Daten	Sicherung von Konfigurationsdaten	Zeitstempel und Zeitsynchronisation	Absicherung von Remote-Zugängen	
sichere Außerbetriebnahme	Time-Out	Sicherung von Nutzdaten			
Manipulations-sicherheit					
DoS-Handling					
Fremdprodukte/ -dienste					

Zentrale Handlungsfelder und zugrundeliegende Anforderungen (Tabelle: VdS)

höchste Sicherheitsanforderungen und Wirtschaftlichkeit durchaus Hand in Hand gehen können. Und eins darf man nicht vergessen: Geschlossen werden müssen die Lücken in den Produkten sowieso. Entweder für die VdS-Prüfung oder nach dem ersten Schaden. Und dass der eintritt, ist sicher.

ETSI TS 103 645 *„Cyber Security for Consumer Internet of Things: Baseline Requirements"*

s+s report: In welchem Verhältnis stehen die VdS-Richtlinien zu anderen Normen und Regelwerken im Bereich der Cyber-Security? Besteht da nicht die Gefahr, dass sich die Anforderungen widersprechen?

Sebastian Brose: Die Richtlinien VdS 3836 stehen inhaltlich in keinem Widerspruch zu Regelwerken, die sich international für den Bereich Cyber-Security in industriellen Anwendungen etabliert haben. Insbesondere zur Normenreihe IEC 62443 besteht eine hohe Kongruenz. So sind die Anforderungen an Komponenten und Systeme in den Richtlinien VdS 3836 in drei unterschiedliche Klassen strukturiert: Klasse A, Klasse B und Klasse C. Diese Nomenklatur entspricht den Anforderungen der Normenreihe IEC 62443 in den Security-Leveln 1–3.

IEC 62443 *„Industrial communication networks – Network and system security"*

Darüber hinaus sind in den Richtlinien VdS 3836 weitere Regelwerke wie beispielsweise das Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) zu den Anforderungen an Smart-Home-Installationen und Geräten des „Internet der Dinge" sowie die ETSI TS 103 645 erfasst.

s+s report: In der Informationstechnik finden bekanntlich neue Entwicklungen in rasantem Tempo statt. Besteht nicht die Gefahr, dass die gerade zertifizierten Produkte schon schnell wieder veraltet und damit unsicher sind?

Sebastian Brose: Wir dürfen Sicherheit nicht mehr als Zustand verstehen, der einmal erreicht wird und dann so bestehen bleibt. Das Zukunftsinstitut hat es treffend so formuliert: „In einer komplex vernetzten Welt, in der sich Bedrohungen und Risiken ständig verändern, ist Sicherheit immer nur punktuell oder phasenweise gegeben. Sicherheit kann somit nicht mehr als ein Endzustand verstanden werden, den es zu erreichen gilt, sondern nur noch als permanenter Prozess, auf den sich Individuen, Organisationen und letztlich die gesamte Gesellschaft bestmöglich einstellen müssen." Dementsprechend sind auch

Unsere Gesprächspartner: Daniel Kaumanns, MBA, (links) ist bei TAS Sicherheits- und Kommunikationstechnik tätig im Produktmanagement Übertragungstechnik und Remote Services sowie verantwortlicher Produktmanager für die TAS Secure Platform; Dipl.-Wirtschaftsjurist (FH) Sebastian Brose (rechts) ist stellvertretender Bereichsleiter und Abteilungsleiter Produktmanagement im Bereich Produkte und Unternehmen bei VdS

die Anforderungen, der Prüf- und Zertifizierungsprozess und die Produktüberwachung für die VdS 3836 abweichend geregelt und neu gedacht.

s+s report: Wie sehen Sie die weitere Entwicklung auf diesem Gebiet?

Sebastian Brose: Die Vernetzung von Systemen und Komponenten der Brandschutz- und Sicherungstechnik hat gerade erst begonnen und wird durch technologische Trends beschleunigt, die in Zukunft erweiterte Anforderungen an die Informationssicherheit stellen. Perspektivisch halten die Richtlinien VdS 3836 auch mit den technologischen Entwicklungen Schritt, die in den kommenden Jahren neue Dimensionen bei der Vernetzung von Systemen und Komponenten der Brandschutz- und Sicherungstechnik einführen werden. Stichwörter in dem Zusammenhang sind KI-basierte Systeme oder selbstüberwachende Systeme, bei denen permanente Prüfungen der Leistungsmerkmale in Echtzeit zum Tragen kommen. All das wird ohne nachgewiesene Cybersicherheit nicht akzeptiert werden. Denn wir dürfen eins nicht vergessen: Die Anlagen werden immer noch einzig und allein zum Schutz von Leib, Leben und Sachwerten installiert!

Daniel Kaumanns: Sicherheitstechnik und IoT sind heute kaum noch trennbar, alles wird immer mehr miteinander vernetzt. Die Sicherheit muss in diesem Kontext neu gedacht werden. Vor diesem Hintergrund werden unabhängige Qualitätsaussagen immer wichtiger. Eine VdS-Zertifizierung – so wie jetzt die gemäß VdS 3836 – ist dabei ein wichtiger Schritt in diese Richtung, für uns und unsere Kunden bleibt VdS ein Garant für Sicherheit.

s+s report: Wir danken Ihnen für dieses Gespräch!

VdS 3836 und SecIoT

Zur besseren Kenntlichmachung der Produkte, die die Anforderungen nach VdS 3836 erfüllen, hat VdS das SecIoT-Logo (s. u.) geschaffen. Weiterführende Informationen zur VdS-zertifizierten Cyber-Sicherheit für vernetzte Produkte, zu den Richtlinien VdS 3836 und zu SecIoT finden Sie unter dem Kurzlink vds.de/3836 oder via QR-Code:

VdS SecIoT