Innovative Methoden der IT-Sicherheit für Kritische Infrastrukturen

Innovative Methoden, mit der Komplexität des Themas IT-Sicherheit Kritischer Infrastrukturen umzugehen, haben sich als ein Schwerpunkt von ITS|KRITS herauskristallisiert. Zu innovativen Methoden und Verfahren für die IT-Sicherheit von Kritischen Infrastrukturen haben mehrere Projekte Vorschläge entwickelt, die sie für den vorliegenden State of the Art vorschlagen:

- Dynamische Maßnahmenkataloge des Projekts Aqua-IT-Lab
- Rollenspezifische Handlungshilfen des Projekts Cyber-Safe
- Spezifische Gefährdungskataloge des Projekts PortSec
- Ermittlung des Sicherheitslevels – vorrangig anhand konkreter Komponenten- und Netzkonfigurationen des Projektes SICIA
- Ermittlungen des Sicherheitslevels – integrierte Betrachtung von Gefährdungen und Sicherheits maßnahmen des Projekts SIDATE

AQUA-IT-Lab: Dynamische Maßnahmenkataloge

Autoren: David Fuhr, Christof Thim

Das Verbundprojekt Aqua-IT-Lab adressiert das Grundproblem – Ressourcenknappheit gerade bei kleinen und mittleren Betreibern Kritischer Infrastrukturen – und macht daraus eine Chance – Kräfte werden durch den dynamischen Maßnahmenkatalog effizient eingesetzt.

Die Methode ist aufwandsarm – es ist für die Betreiber Kritischer Infrastrukturen keine Aufwandsanalyse notwendig. Aqua-IT-Lab hat es sich zum Ziel gesetzt, dass kleine Betreiber um die Risikoanalyse herumkommen. Dies konnte auf zwei Wegen erfolgen: Erstens musste ähnlich wie im Grundschutz die Bedrohungsanalyse allgemein a priori vorgenommen werden – denn die Voraussetzungen, wie Akteure, zeitliche Entwicklung der Bedrohungslage, grobe Typen von Prozessen, Anlagen und Technik – sind bei kleinen Betreibern ähnlich. Zweitens waren für die typischen Prozesse und Installationen allgemeine Maßnahmen nach Stand der Technik für den passenden Schutzbedarf – hoch bis sehr hoch – zu entwickeln. Beides konnte geleistet werden durch die Analyse diverser einschlägiger Bedrohungs- und Maßnahmenkataloge, Standards und Richtlinien sowie durch die in Aqua-IT-Lab entwickelten Self-Assessments. Kernstück der Methode ist die automatische Erzeugung von Maßnahmen. Um in der Ressourcenschonung noch einen Schritt weiterzugehen, haben wir uns entschlossen, auch den Schritt der Umsetzungsüberprüfung der Maßnahmen (BSC, siehe oben) zu integrieren und halbautomatisch ausführen zu lassen. Zu dem Zweck wurde das Self-Assessment um die automatische Generierung von Handlungsempfehlungen, also High-Level-Maßnahmen, erweitert. Dem zugrunde liegt ein umfangreicher Maßnahmenkatalog, der jedoch nie in Gänze ausgegeben wird, um einen Abschreckungseffekt und Demotivation zu vermeiden, sondern immer gemäß der aktuell geltenden Selbsteinschätzung über 11 Themenfelder die ressourcenoptimal jeweils schutzmaximierenden/risikominimierenden nächsten Maßnahmen berechnet.

Input: Self-Assessment

Der erste Schritt ist ein Self-Assessment. Die folgenden Themenfelder werden im Self-Assessment nach Umsetzungs- („nicht umgesetzt“ bis „trifft voll zu und wurde überprüft“) sowie Dokumentationsgrad („nicht dokumentiert“ bis „vollständig dokumentiert und regelmäßig aktualisiert“) eigenständig bewertet:

Abb. 3: Themenfelder des Self-Assessment

Das Resultat des Self-Assessment ist eine Abschätzung des Reifegrads der existierenden Maßnahmen mit einer Abschätzung des Restaufwands und der Minima des Reifegrads. Diese dienen der Erkennung der größten Risiken (vgl. Abb. 4).

Abb. 4: Auswertung des Reifegrads mit Reifegrad und Minima

Auswertung - Reifegrad

Thema	Praxis - Minimum	Praxis - Reifegrad	Doku - Minimum	Doku - Reifegrad
1 - Organisation	0%	49%	33%	62%
2 - Dokumentation und Zonen	40%	60%	33%	67%
3 - Datenübertragung	20%	33%	33%	44%
4 - Berechtigungsmanagement	40%	55%	33%	58%
5 - Outsourcing & Fernadministr.	40%	56%	33%	60%
6 - Schadsoftware & Schwachstellen	40%	56%	33%	47%
7 - Wechseldatenträger & mobil	20%	50%	33%	50%
8 - Komponentenlebenszyklus	20%	51%	33%	48%
9 - IT-Störungsmanagement	40%	55%	33%	42%
10 - Notfallplanung	20%	50%	33%	67%
11 - Audit	60%	67%	67%	67%
Gesamtergebnis	0%	53%	33%	56%

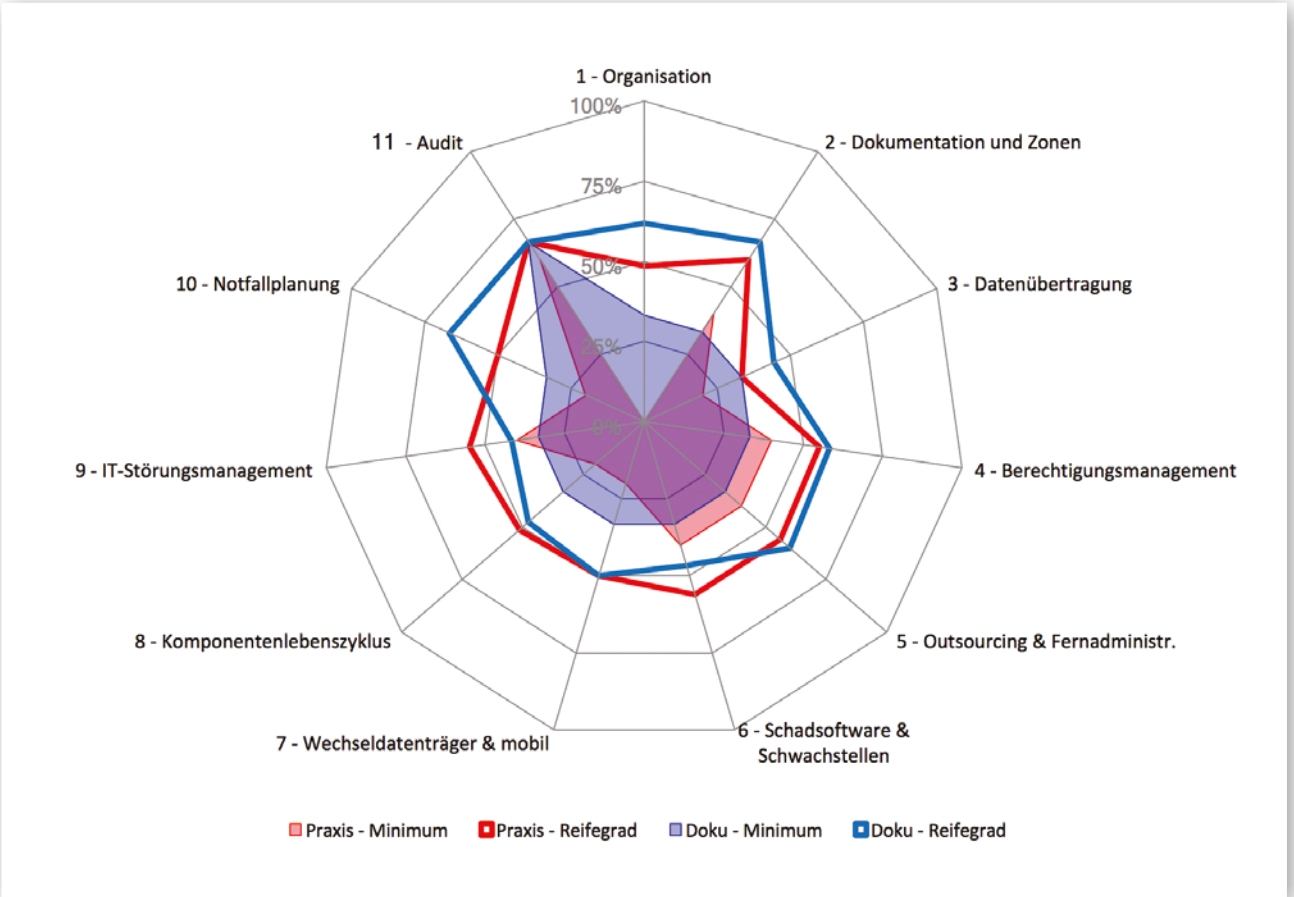
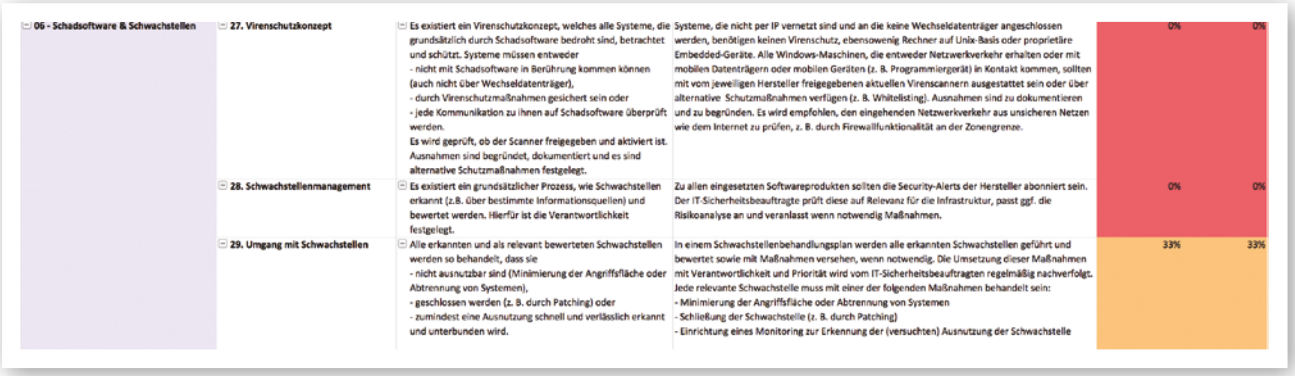


Abb. 5: Darstellung der Ergebnisse des Self-Assessments

Output: generierte Handlungsempfehlungen

Aus den Ergebnissen des Self-Assessment generiert das System automatisch eine Liste von Handlungsempfehlungen, die in ihrer Priorisierung (Reihenfolge) den optimalen Pfad abbilden, um ressourcensparend den Security-Reifegrad der Themen mit den größten Risiken sukzessive anzuheben.



06 - Schadsoftware & Schwachstellen	27. Virenschutzkonzept	Es existiert ein Virenschutzkonzept, welches alle Systeme, die grundsätzlich durch Schadsoftware bedroht sind, betrachtet und schützt. Systeme müssen entweder - nicht mit Schadsoftware in Berührung kommen können (auch nicht über Wechseldatenträger), - durch Virenschutzmaßnahmen gesichert sein oder - jede Kommunikation zu ihnen auf Schadsoftware überprüft werden. Es wird geprüft, ob der Scanner freigegeben und aktiviert ist. Ausnahmen sind begründet, dokumentiert und es sind alternative Schutzmaßnahmen festgelegt.	Systeme, die nicht per IP vernetzt sind und an die keine Wechseldatenträger angeschlossen werden, benötigen keinen Virenschutz, ebensowenig Rechner auf Unix-Basis oder proprietäre Embedded-Geräte. Alle Windows-Maschinen, die entweder Netzwerkverkehr erhalten oder mit mobilen Datenträgern oder mobilen Geräten (z. B. Programmiergerät) in Kontakt kommen, sollten mit vom jeweiligen Hersteller freigegebenen aktuellen Virenscannern ausgestattet sein oder über alternative Schutzmaßnahmen verfügen (z. B. Whitelisting). Ausnahmen sind zu dokumentieren und zu begründen. Es wird empfohlen, den eingehenden Netzwerkverkehr aus unsicheren Netzen wie dem Internet zu prüfen, z. B. durch Firewallfunktionalität an der Zonengrenze.	0%	0%
	28. Schwachstellenmanagement	Es existiert ein grundsätzlicher Prozess, wie Schwachstellen erkannt (z.B. über bestimmte Informationsquellen) und bewertet werden. Hierfür ist die Verantwortlichkeit festgelegt.	Zu allen eingesetzten Softwareprodukten sollten die Security-Alerts der Hersteller abonniert sein. Der IT-Sicherheitsbeauftragte prüft diese auf Relevanz für die Infrastruktur, passt ggf. die Risikoanalyse an und veranlasst wenn notwendig Maßnahmen.	0%	0%
	29. Umgang mit Schwachstellen	Alle erkannten und als relevant bewerteten Schwachstellen werden so behandelt, dass sie - nicht ausnutzbar sind (Minimierung der Angriffsfläche oder Abtrennung von Systemen), - geschlossen werden (z. B. durch Patching) oder - zumindest eine Ausnutzung schnell und verlässlich erkannt und unterbunden wird.	In einem Schwachstellenbehandlungsplan werden alle erkannten Schwachstellen geführt und bewertet sowie mit Maßnahmen versehen, wenn notwendig. Die Umsetzung dieser Maßnahmen mit Verantwortlichkeit und Priorität wird vom IT-Sicherheitsbeauftragten regelmäßig nachverfolgt. Jede relevante Schwachstelle muss mit einer der folgenden Maßnahmen behandelt sein: - Minimierung der Angriffsfläche oder Abtrennung von Systemen - Schließung der Schwachstelle (z. B. durch Patching) - Einrichtung eines Monitoring zur Erkennung der (versuchten) Ausnutzung der Schwachstelle	33%	33%

Abb. 6: Generierte Handlungsempfehlungen (Auszug)

Für den Betreiber Kritischer Infrastrukturen, der diese Methode wählt, bleiben im Wesentlichen folgende Aufgaben:

1. Verifizierung der Priorisierung mit der Leitungsebene
2. Planung der Umsetzung und Ressourcen über die Zeit
3. Konkretisierung der Handlungsempfehlungen für die eigenen Rahmenbedingungen
4. Umsetzung der geplanten Maßnahmen

Insbesondere bei letzterem Punkt kann das Vorgehensmodell nur unterstützen. Bei den Punkten 2 und 3 sollte in der Regel die Hilfe eines Beraters für eine effiziente Umsetzung hinzugezogen werden.