Mehr Datenschutz und Betriebssicherheit durch Cyber-Security-Testing

Eine Anleitung zur Cyber-Defense-Benchmarking und Vulnerability-Analyse in Unternehmen und Organisationen.

Cyber-Security wird für Unternehmen wie auch für die Politik immer mehr zu einem kritischen Thema, denn Cyber-Angriffe, Wirtschaftsspionage und Datenmissbrauch können eine existenzbedrohende Gefährdung darstellen. Vor diesem Hintergrund gründete im Jahr 2009 der französische IT-Sicherheitsexperte Gérard Gaudin den Club R2GS (Réflexion et Recherche en Gestion opérationnelle de la Sécurité) mit dem Zweck, Wissen und Erfahrungen aus den unterschiedlichsten Branchen zu nutzen, um spezifische europäische Sicherheitsstandards zum Schutz vor Cyber-Kriminalität in Unternehmen, Behörden und Organisationen zu entwickeln. Der Club mit mehr als 150 Mitgliedern aus rund 40 namhaften Unternehmen und Einrichtungen der EU, operiert europaweit und hat sog. R2GS-Chapters in Frankreich, Großbritannien, Deutschland, Italien, Luxemburg und Belgien gegründet.

Das deutsche Chapter „Club R2GS-SoSo“ unter der Leitung von Jan de Meer und Axel Rennoch gibt es seit 2012. Das Ziel der Club-Mitglieder ist die Erarbeitung einer Handlungsanleitung zum Aufbau digitaler Sicherheitsarchitekturen in mittelständischen Dienstleistungsunternehmen, gestützt auf Empfehlungen und Normen des „European Telecommunication Standardization Institute (ETSI)“ sowie nationaler Einrichtungen wie z.B. DIN, BSI und VDI.

Gemeinsam mit seinen Kollegen Jens Richter und Axel Rennoch beantwortet Jan deMeer SQ-Fragen zum Thema Cyber-Security-Testing und gibt Handlungsempfehlungen zur Cyber-Defense-Benchmarking- bzw. Vulnerability-Analyse in Unternehmen.

SQ: Welche Strategien und Lösungsansätze zum Schutz der Informations- und Kommunikationstechnik (IKT)-Infrastrukturen sehen Sie und welche Wege schlagen Sie vor?

IKT-Sicherheit betrifft alle Wirtschafsbetriebe, z.B. in den Sektoren Logistik, Finanzen, Verkehr, Elektrogewerbe, Energie, IKT/Cloud Computing, Technischer Messtechnik, aber auch Juristen, Forschungseinrichtungen und Behörden. Die Bandbreite und die Aktivitäten sind so vielseitig und umfassend, dass sich alle Beteiligten auf ihre zentralen Aufgaben fokussieren müssen. Aus Sicht eines Forschungsinstituts wie Fraunhofer FOKUS gehören dazu insbesondere Forschungsprojekte zum modell- und risiko-basierten Sicherheitstesten, Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) konzentrieren sich u.a. auf Produktzertifizierungen nach Common Criteria [5], die Firmen orientieren sich an Standardisierungsarbeiten

und organisieren sich z. B. in Interessenverbänden wie der Allianz für Cybersicherheit des BSI, den Security-Fachgruppen der GI und natürlich dem ASQF. Jeder Beitrag ist wichtig.
Zu den wichtigen Ergebnissen zählen wir Qualitätsprüfungen, z.B. eine möglichst automatisierte Herleitung und Ausführung von Sicherheitstests, u.a. aus Modellen der hochkritischen Software-Anteile (z.B. unter Verwendung innovativer Fuzzing Methoden). Wir halten viel von sicherheitstechnischen Produktprüfungen, die von der Begutachtung einer Entwicklungsumgebung bis zur Anerkennung internationaler Sicherheitszertifikate reichen. Und wir setzen auf die Erarbeitung und Anwendung von Standards zur Messung von Sicherheit in großen und kleinen Betrieben. Gerade der letzte Aspekt ist noch nicht in ausreichendem Maße erarbeitet bzw. gelöst worden und steht im Mittelpunkt der Arbeiten vom Club R2GS.

SQ: Der Club R2GS strebt eine Sammlung von Sicherheitsindikatoren und den Austausch von Praxiswissen aus Security-Operation-Centern (SOC) über Normungs- und Rechtsgrundlagen zum sicheren Betrieb der IKT in Unternehmen unterschiedlicher Branchen an. Wie beurteilen Sie die aktuelle Bedrohung durch Cyber-Kriminalität?

Das eine ist die Gefahr aus dem Netz, das andere ist die Verletzlichkeit (vulnerability) unserer IKT-Systeme und Infrastrukturen. Während das BSI mit Recht vor Angriffen warnt, versucht der Club R2GS, Maßstäbe (Indikatoren) zu finden, um die Verletzlichkeit der IT zu messen – ggf. auch in Echtzeit während des Betriebs (resiliency) – damit passende Maßnahmen bei jeder Gefährdungslage zeitnah ergriffen werden können.
Das BSI hält in seinem Register aktueller Cyber-Gefährdungen und Angriffsformen sechs besonders bedrohliche relevante Formen fest, darunter: das gezielte Hacking von Webservern; Drive-by-Exploits zur Kontaminierung von Rechnern mit Schadsoftware per E-Mail oder beim Surfen; Distributed-Denial-of-Service-Angriffe per Botnetze; Schad-Software mittels SPAM oder Identitätsdiebstahl und die Kompromittierung von zentralen Sicherheitsinfrastrukturen. Diese Formen der Gefährdung sind alltäglich und können daher zu jedem Zeitpunkt, in jedem Unternehmen oder bei jeder Inanspruchnahme digitaler (Cloud-) Dienstleistungen auftreten.

SQ: Welche Bedeutung haben die Information-Security-Indicators (ISI) für den Schutz der IKT-Infrastrukturen in Unternehmen und Organisationen?

Zwischen der industriellen Normungsgruppe „ETSI ISG Information Security Indicators (ISI)“ [1], unterstützt durch den mit ihr verbundenen Club R2GS, und der internationalen Normungsgruppe „ISO/IEC SC27 WG4 Security controls and services“ besteht eine formale Normungs-Liaison [10, 11] zur Entwicklung von ISI-gestützten Methoden zur Evaluation der Cyber-Sicherheit und Cyber-Defense.
Der Club R2GS [3] ist ein Zusammenschluss – außerhalb der Normungsorganisationen – von privaten und öffentlichen Organisationen, Unternehmen und Dienstleistern aus allen möglichen Branchen, die ein Security-Operation-Center (SOC) oder ein Security-Incident-Response-Team (SIRT) [12, 13] zur Kontrolle ihrer IKT-Infrastrukturen betreiben oder beraten.
Die nationalen Gliederungen vom R2GS unterstützen die Verbreitung von Verfahren und Zielen von Sicherheitsnormen und Industriestandards zur Evaluierung kritischer IKT/Daten-Infrastrukturen oder SOCs, um sie vor Zerstörung, Missbrauch oder Veränderungen zu schützen; aber auch, um Sicherheit, Zuverlässigkeit, Wirtschaftlichkeit oder Wettbewerbsfähigkeit der verwendeten Technologien zu steigern.

SQ: Welchem Zweck dient das normierte SIEM-Referenz-Modell?

Das „Security Information and Event Management“ (SIEM) -Modell [9] beschreibt ähnlich dem Phasenmodell „Information Security Incident Management (ISIM)“ [7] die Auswertung von beobachteten Sicherheitsereignissen in fünf Schritten. Es dient daher zur Überprüfung von Sicherheitserfordernissen. Das SIEM- wie das ISIM-Modell ist ereignisorientiert und stützt sich auf das sog. Publish-Subscribe-Kommunikations-Paradigma, in welchem alle Ereignisse einer bestimmten Domäne, z.B. alle spezifizierten Sicherheitsindikatoren des SIRT/SOC eines Unternehmens, verwaltet werden.
Im SIEM-Modell gibt es, neben Ereignis, Beobachter und Bekanntgeber (-Objekten), eine weitere Funktionalität bzw. Rolle, die von Analysten (-Objekten) ausgeführt wird. Die Analystenrolle zeichnet sich darin aus, zum Einen zu entscheiden, welche Maßnahmen aufgrund kritischer Sicherheitsereignisse ergriffen werden müssen und zum Anderen zu kontrollieren, welche Wirkung die ergriffene Maßnahme auf das beobachtete sicherheitsrelevante Ereignis hat.

SQ: Was sind normierte Beschreibungselemente zur Spezifikation von Ereignisinformationen?

Jedes Ereignis ist Träger konkreter Informationen, welche mittels sog. SIEM-„Deskriptoren“ in standardisierter Form beschrieben werden. Davon getrennt ist die Interprozess-Kommunikation zu betrachten: Beobachtung und Erzeugung von Ereignissen müssen „mandanten-spezifisch“ (vgl. Bundesdatenschutzgesetz) abgewickelt werden, in dem die Ereignisse, in sog. Ereignisklassen voneinander getrennt, behandelt werden.

Ein Beispiel: Intrusion-Indikator-Spezifikationen bestehen i.d.R. aus drei Beschreibungsebenen: der definitorischen (category, correspondence, ▶

definition), der operativen (frequency, securityLevel, detectionMeans, detectionLevel) und der evaluatorischen Ebene (indicatorProduction, indicatorValue, KPSImaturity, benchmarking). Die Werte der Deskriptoren korrespondieren mit den Beobachtungen bzw. Messwerten des Systemzustands im SIEM-Modell. Erforderliche Maßnahmen, die sich aus der Evaluation ergeben, korrespondieren mit der Anwendung von Steuerungsmaßnahmen und der zyklischen Beobachtung ihrer Wirkung.

SQ: Wie kann ein allgemeines Anwendungsschema für ETSI-Sicherheitsindikatoren aussehen?

ISI-Indikatoren stehen Unternehmen und Organisationen mit den bei ETSI publizierten Spezifikation ETSI GS ISI 001 [1] zur Verfügung. Für die strukturierte Darstellung der Indikatoren ist ein den „Common Criteria"[5] entlehntes Klassifikationsschema angewendet worden: Die Indikatoren sind in Bäumen mit den fünf Ebenen Oberklassen, Klassen, Familien, Komponenten und Parameter dargestellt. Es gibt die drei Oberklassen Incidents, Vulnerabilities sowie Impacts, die mittels den entsprechenden Bezeichnern „Ixx", „Vxx" und „IMP" unterschieden werden.

Die Oberklasse **„Incidents"** enthält vier Klassen:

- IEX: Intrusion and external attacks (Eindringversuche und Angriffe von außen);
- IMF: Malfunctions (Fehlverhalten);
- IDB: Internal deviant behaviours (organisationsinternes, auffälliges Verhalten);
- IWH: Whole incident categories (sonstige Vorfälle).

Die Oberklasse **„Vulnerabilities"** enthält fünf Klassen:

- VBH: Behavioural vulnerabilities (Angriffsfläche seitens des [System-] Verhaltens);
- VSW: Software vulnerabilities (Angriffsfläche seitens der Software);
- VCF: Configuration vulnerabilities (Angriffsfläche seitens der Konfiguration
- VTC: General security technical vulnerabilities (Angriffsfläche seitens der Technologie);
- VOR: General security organizational vulnerabilities (Angriffsfläche seitens der (Betriebs-) Organisation).

Die Oberklasse **„Impacts"** beinhaltet nur die Klasse „IMP – Impact Measurement" (Maß für die Auswirkung eines Vorfalls).

Klassen beinhalten Familien von Komponenten, die eine Anzahl von Parametern besitzen können. Zum Beispiel beinhaltet die Familie „VBH_HUW: Behavioural Vulnerabilities - Human Weaknesses" folgende zwei Komponenten (s. Abb.):

1 Ausspähen nach Anklicken von Internet-Links oder Öffnen von Mailanhängen.

2. Indicators with vulnerabilities (Vxx)

CLASS	FAMILY			COMPONENT AND IDENTIFIER	PARAMETERS	F	S	D
VBH Behaviour vulnerabilities	PRC	Dangerous protocols used	1	Server accessed by an admin with unsecure protocols	#ev[30d], #admins.system[30d], Ømonth[90d]	sig	2-3	1
			2	P2P client in a workstation	#users.installing[30d], Ømonth[90d]	++	3	2
			3	VoIP client in a workstation	#users.installing[30d], Ømonth[90d]	++	1	2
			4	Outbound connection dangerously set up	#users.installing[30d], Ømonth[90d]	++	2	2
			5	Not compliant lap top computer used to establish a connection	#users.connecting[30d], #laptops, Ømonth[90d]	++	3	2
			6	Other unsecure protocols used	#ev[30d], Ømonth[90d]	+	2-3	1-2
	IAC	Internet illicit access	1	Outbound controls bypassed	#users.performing[30d], Ømonth[90d]	sig	2-4	1
			2	Anonymisation site used	#users.performing[30d], Ømonth[90d]	sig	3	3
	FTR	File illicit transfer with outside	1	File recklessly downloaded	#ev[30d], Ømonth[90d]	++	2-3	2
			2	Personal public instant messaging account used (for business file exchanges)	#users.performing[30d], Ømonth[90d]	+	3	2
			3	Personal public messaging account used (for business file exchanges)	#users.performing[30d], Ømonth[90d]	sig	2	2
	WTI	Workstation used w/o relevant usual security	1	Workstation with a disabled or not updated AV and/or FW	#users.performing[30d], #org.workstations, Ømonth[60d]	+	4	3
			2	Workstations accessed in admin mode	#users.performing[30d], Ømonth[60d]	+	2-3	2
			3	Personal storage devices used	#ev[30d], Ømonth[90d]	++	3	1
			4	Personal devices used w/o compartmentalization (BYOD)	#users.performing[30d], #devices.personal, Ømonth[90d]	++	2	1
			5	Not ciphered sensitive files exported	#ev[30d], Ømonth[90d]	++	4	1
			6	Personal software used	#users.performing[30d], Ømonth[60d]	+	2-3	3
	PSW	Passwords illicitly handled or managed	1	Weak passwords used	#ev[30d], #accounts.users, Ømonth[90d]	sig	3	2
			2	Passwords not changed	#ev[30d], #accounts.users, Ømonth[90d]	sig	2	2
			3	Admin passwords not changed	#ev[30d], #accounts.admins, Ømonth[90d]	sig	3	2
	RGH	Access rights illicitly granted	1	No compliant user rights granted by admin	#admins.performing[30d], #admins, Ømonth[90d]	?	3	2
	HUW	Human weakness	1	Exploited by spear phishing message (links/attachments)	#users.performing[month], #users, Ømonth[90d]	+	3	2
			2	By exchanges secrets (phone/f2f)	#users.performing[month], #users, Ømonth[90d]	+	1	1-2
VSW Software vul.	WSR	Webserver sw. vul.	1	Web applications sw vul.	#ev[30d], #applications.web, Ømonth[90d]	+	3-4	3
	OSW	OS sw. vul	1	OS sw vul. regarding servers	#ev[30d], #server.ext.visible, Ømonth[90d]	+	2-3	3
	WBR	Webbrowser sw. vul.	1	Webbrowser sw. vul.	#ev[30d], #workstations, Ømonth[90d]	++	2-4	3

Abbildung: Die Indikatoren der Familie VBH_HUW [Q2]

2 Ausspähen bei Telefonaten oder anderen Besprechungen.

Beide Komponenten errechnen sich unter Einbeziehung folgender Parameter: Anzahl der betroffenen Benutzer, Anzahl aller Benutzer sowie die durchschnittliche Anzahl der Beobachtungen in einem Zeitraum von 90 Tagen. Zusätzlich wird jede ISI-Komponente durch die folgenden Kennzahlen bewertet: Frequenzrate, Gewichtung der Wirkung sowie Aufwand für die Aufspürung.

SQ: Welche Schlussfolgerungen ziehen Sie aus den Anwendungsschemata für die Sicherheit der IKT-Infrastruktur in Unternehmen und Organisationen?

Benchmarking unter Verwendung des ISI-Katalogs kann von kleinen und mittelständischen Unternehmen oder anderen Organisationen zur (Selbst-) Bewertung ihrer (kritischen) IKT-Infrastruktur herangezogen werden. Dabei werden zwei Verfahren unterschieden: Erstens, das auf Kennzahlen und zweitens, das auf Erwartungswerten gestützte Messverfahren:
Man spricht von einem kennzahlgestütztem Verfahren, wenn ein Bündel von ISI-Kennzahlen wie ein Index gestaltet wird. Dabei ist die verglichene aktuelle IKT-Infrastruktur gleich, besser oder schlechter als ein allgemeiner Vergleichswert. Der verantwortliche SIRT/SOC-Manager kann aus diesem Vergleich seine eigenen Schlüsse über die Sicherheit der betrachteten Infrastruktur ziehen.
Die zweite Art der Bündelung prüft einen bestimmten Erwartungswert, z.B. die Vermutung, dass Eindringversuche in die IKT-Infrastruktur eines Unternehmens an bestimmten Schnittstellen (z.B. Browsern) erfolgreicher ablaufen als mit anderen. Dies kann auch mit einem geeigneten Bündel von ISI-Komponenten untersucht werden und die Vermutung dadurch bestätigen oder entkräften.

Benchmarking unterstützt auch die Bewertung von Maßnahmen zur Stärkung der Widerstandskraft (Resilienz) eines Unternehmens bzw. Systems gegenüber Angriffen auf die IKT-Infrastruktur oder Destabilisierung eines Systems aufgrund offener, d.h. nicht indizierter, Schwachstellen.

> Bitte wenden Sie sich bei Interesse an den beschriebenen Themen an das deutsche Chapter vom Club R2GS [4]. Wir freuen uns auf Ihre Mitarbeit.
>
> *Jan de Meer*

Ein besonders sensibler Bereich in einem Unternehmen ist ggf. die Sicherung der Produktion von Waren oder der Ressourcen zur Bereitstellung einer Dienstleistung, z.B. der Betrieb eines Cloud-Computing-Data-Centers. Der Club R2GS-SoSo stützt sich u.a. auf folgende vier Säulen bzw. Modelle: Informations-Akquise-Modell, vertrauen-schaffendes Rollenmodell, Regelkreis-gestützte Sicherheitsarchitekturen und Informationszusicherungs- und Compliance-Modell. Hier werden die formalen Aspekte der Modellbildung beschrieben [12,13] sowie das zugrundeliegende „Cyber-Defense und Security Modell", das sich auf die vier Säulen stützt, anhand von Position-Statements erklärt [14].
International sind die Definition und Klassifikation der Sicherheits-Indikatoren in methodische Normungsprojekte eingebettet und vom Club R2GS begleitet: „Information Security Management"[6], „Information Security Incident Management"[7], „Selection, Deployment and Operations of Intrusion Detection and Prevention Systems"[8], „Guidelines for Security Information and Event Management"[9]. ■

Quellen: **[1]** ETSI ISG Information Security Indicators (ISI) http://www.etsi.org/images/files/ETSITechnologyLeaflets/InformationSecurityIndicators.pdf **[2]** ISI Quick Reference Card: Wikipedia "Information Security Indicators", https://en.wikipedia.org/wiki/Information_security_indicators, s. "External links". **[3]** R2GS Europe: http://www.linkedin.com/groups/Club-R2GS-4725685/about **[4]** R2GS-SoSo Deutschland: http://www.school-of-technology.de/7.html **[5]** Common Criteria: https://www.commoncriteriaportal.org, http://www.school-of-technology.de/resources/ccQRC.pdf

ISO Quellen: **[6]** ISO/IEC 27004:2009 IT Security techniques- Information security management (ISM) – Measurements; **[7]** ISO/IEC 27035 (WD 2013) IT Security techniques – Information security incident management; **[8]** ISO/IEC 27039:2006 IT Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS); **[9]** ISO/IEC 27044 (WD 2012) IT Security techniques – Guidelines for Security Information and Event Management (SIEM); **[10]** ISO/IEC JTC1/SC27 N12739: Resolutions of the 25th SC 27 Plenary meeting held in Sophia Antipolis, France, 29th – 30th April 2013, Resolution 19 „Liaison Statements " und Resolution 20 „Appointment of Liaison Officers" **[11]** ISO/IEC JTC1/SC27 WG4 N12638: ETSI ISG ISI Liaison Request, 2013

White Papers (www.school-of-technology.de): **[12]** Claudia Ermel, TUB, Jens Richter, Jan deMeer, ssl.eu GmbH: „Regel-gestützte Modellierung von Anwendungsszenarien Kritischer Infrastrukturen für Analyse und Ausbildung" **[13]** Jan deMeer, ssl.eu GmbH: „Model-driven Safe & Secure Operation of a Virtual Power Plant" (Industrie4.0), eingereicht zum FINESCE Open Call; **[14]** Jan deMeer, ssl.eu GmbH BEST IT2Energy Position Statements: PS01 Energie Lastprofilierung; PS02 Energiefluß-Steuerung; PS03 KRITIS Teilhabermodell; PS04 Maßnahmekatalog Energie-Effizienz;

Jan de Meer ist Geschäftsführer der smartspacelab.eu GmbH.

Axel Rennoch ist Projektleiter am Fraunhofer Institut FOKUS.

Jens Richter ist Freiberufler im Bereich mobile Applikationen.