# Vorhersage der Cyber-Resilienz einer Organisation durch Emulation der Geschäftsprozesse und des Laufzeitverhaltens von IT/OT-Infrastrukturen

Marcel Kühne, Oliver Nitschke

Fraunhofer IOSB, Institutsteil Angewandte Systemtechnik (AST), Abteilung Kognitive Energiesysteme (KES), Gruppe IT-Sicherheit für Energie- und Wasserversorgung, Wilhelmsplatz 11, 02826 Görlitz

**Abstract**

Cyber-Resilienz ist ein entscheidender Faktor für die Widerstandsfähigkeit einer Organisation im Bereich der IT/OT-Sicherheit und beschreibt ihre Fähigkeit, IT/OT-Störungen zu widerstehen und sich davon zu erholen. Ein weit verbreiteter Ansatz zur Messung der Cyber-Resilienz sind Cyber-Resilienz-Metriken. Deren Datenbasis beschränkt sich nicht nur auf die Erfassung sicherheitskritischer Vorfälle in der IT/OT-Infrastruktur, sondern umfasst auch die organisatorische Prozessebene sowie die dahinter liegenden Abläufe beim Auftreten sicherheitsrelevanter Ereignisse im Unternehmen. Eine umfassende Aussage zur Cyber-Resilienz ist erst nachgelagert möglich, da sie direkt abhängig von der Verfügbarkeit ausreichend qualitativer Daten über einen längeren Zeitraum ist. Dazu zählen unter anderem der Umgang einer Organisation mit Sicherheitsmeldungen, die Durchführung von Patchprozessen, das Auftreten von Cyber-Angriffen sowie die Reaktion auf derartige Sicherheitsvorfälle. Fehlt diese Datenbasis, kann eine Aussage zur Cyber-Resilienz nicht oder nur eingeschränkt getroffen werden.

In diesem Beitrag wird ein modellbasierter Ansatz vorgestellt, der es ermöglicht, ohne langfristige Datenerfassung eine qualitative Aussage über die Cyber-Resilienz einer Organisation und ihrer IT/OT-Infrastruktur zu treffen. Dabei werden neben der technischen Infrastrukturebene auch alle relevanten organisatorischen Prozessschritte abgebildet. In dieser Umgebung können unterschiedliche Ereignisse und deren Auswirkungen auf die Cyber-Resilienz über verschiedene Zeiträume emuliert werden. Sie ermöglicht die Einbindung von Cyber-Resilienz-Metriken mit Bezug zu den organisatorischen Geschäftsprozessen. Darüber hinaus können ereignisbasierte Cyber-Resilienz-Metriken präventiv eingesetzt werden, da ihre Abhängigkeit von tatsächlichen IT-Sicherheitsvorfällen entfällt. Dies führt zu einer Vorhersagefähigkeit der Cyber-Resilienz für eine Organisation.

Stichworte: Cybersicherheit, Resilienz, Metrik, Emulation, Vorhersage

## 1. Einführung

Cyber-Resilienz bezeichnet die "Fähigkeit [einer Organisation], sich anzupassen und den Geschäftsbetrieb fortzusetzen und Ziele zu erreichen, unabhängig von Cybervorfällen"[1] (Greiman & Bernardin, 2021). Die primären Ziele sind die Prävention, Bewältigung und Erholung von sicherheitsrelevanten Cyberereignissen. Konzeptionell werden dabei die beiden Bereiche Informationssicherheit mit ihren Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit einerseits sowie Geschäftskontinuität und organisatorische Belastbarkeit andererseits zusammengeführt. Im Fokus stehen vor allem die technische Infrastruktur, also die Informationstechnologie (IT) und Operative Technologie (OT), sowie die organisatorische Prozessebene, also die nachgelagerten Prozesse beim Auftreten sicherheitsrelevanter Ereignisse. In diesem Zusammenhang ist die Einschätzung der eigenen Cyber-Resilienz für eine Organisation elementar, d. h. deren Messung für die Analyse, Bewertung und Anpassung von Maßnahmen zur Steigerung der Widerstandsfähigkeit gegenüber IT/OT-Störungen. Zu diesem Zweck werden häufig Cyber-Resilienz-Metriken verwendet.

*Problem*

Der Einsatz bzw. die Bewertung von Cyber-Resilienz-Metriken setzt das Auftreten von Cybervorfällen in quantitativer und qualitativer Hinsicht voraus. Dies wiederum bedeutet in der Praxis die Beobachtung und Erfassung von Messwerten über einen längeren Zeitraum. Grundsätzlich führt dieser Umstand zu der Problematik, dass eine umfassende Aussage zur Cyber-Resilienz auf Basis entsprechender Metriken erst nachgelagert möglich ist, d. h. Ergebnisse und Auswertungen liegen in der Regel erst nach einer langfristigen Beobachtungsdauer vor, wobei dadurch die quantitativen oder qualitativen Anforderungen nicht automatisch erfüllt sind. Infolgedessen ergeben sich verzögerte Aussagen zur Wirkung von Cyber-Resilienz-Maßnahmen, da eine zeitnahe Evaluierung der Maßnahmeneffektivität nicht möglich ist. Zusätzlicher Aufwand entsteht durch die Etablierung mittel- bis langfristiger Evaluierungsprozesse für die Cyber-Resilienz.

*Hypothese*

Von Vorteil wäre die Einschätzung der Widerstandsfähigkeit einer Organisation gegenüber sicherheitsrelevanten Cyberereignissen ohne die bisher damit verbundenen Nachteile. Die daraus resultierende Prognosefähigkeit der Cyber-Resilienz betrifft neben der technischen Infrastrukturebene (IT/OT-Infrastruktur) auch alle damit verbundenen organisatorischen Prozessschritte. Das Ziel ist eine qualitative Aussage über die Cyber-Resilienz einer Organisation mittels Cyber-Resilienz-Metriken ohne die übliche langfristige Datenerfassung. Folgende Hypothese wird formuliert:

*Die Cyber-Resilienz einer Organisation kann durch Emulation ihrer Geschäftsprozesse sowie des Laufzeitverhaltens ihrer IT/OT-Infrastruktur mittels Cyber-Resilienz-Metriken vorhergesagt werden.*

[1] *"ability to adapt and continue business operations and accomplish objectives, regardless of the cyber incidents"*

*Verwandte Arbeiten*

Die hier vorgestellten Arbeiten beziehen sich auf die Abbildung von Geschäftsprozessen sowie die Darstellung technischer IT/OT-Infrastrukturen mittels Emulation. In Siaterlis et al. (2011) wird ein angepasstes Emulab-basiertes Testbed als Emulationsumgebung für Cyberübungen vorgestellt. Siaterlis et al. (2013) zeigen die Eignung von Emulationsumgebungen auf Basis der Software Emulab für die Durchführung wissenschaftlicher Experimente hinsichtlich der Eigenschaften Experimenttreue, Reproduzierbarkeit, Messgenauigkeit und Störungen sowie der damit verbundenen repräsentativen Abbildung des Verhaltens realer Systeme. Die Modellierung der Auswirkungen potenzieller Cyberangriffe auf die Prozessabläufe von (militärischen) Systemen wird sowohl in Musman et al. (2013) basierend auf der Business Process Model and Notation (BPMN) als auch in Lang & Madahar (2017) auf der Basis der Unified Modeling Language (UML) dargestellt. In Kott et al. (2018) werden mit *metric-based* und *model-based* die zwei primären Ansätze zur Quantifizierung der Resilienz beschrieben.

*Thematische Eingrenzung*

Der grundlegende Absatz sowie die Bewertung der Cyber-Resilienz basieren auf Cyber-Resilienz-Metriken. Eine Evaluierung dieser hinsichtlich ihrer grundsätzlichen Eignung, Vollständigkeit oder eventueller Unzulänglichkeiten zur Beurteilung der Cyber-Resilienz ist nicht Bestandteil dieses Beitrags.

*Gliederung*

Der vorliegende Beitrag ist wie folgt aufgebaut: Abschnitt 2 erklärt das Vorgehensmodell und die methodische Herangehensweise. In Abschnitt 3 werden die Ausarbeitungen vorgestellt. Die Darstellung der wichtigsten Erkenntnisse sowie eine Interpretation der Ergebnisse erfolgen in Abschnitt 4. Mögliche Erweiterungen des Ansatzes werden in Abschnitt 5 zusammengefasst.

## 2. Vorgehensmodell

Die Vorgehensweise basiert auf der Design Science Research (DSR) Methodologie, einem gestaltungsorientierten Ansatz. Konzeptionell wird in diesem Beitrag nicht von einer möglichst exakten Abbildung des Vorbildes, also der Simulation der Infrastruktur sowie der Geschäftsprozesse einer Organisation, ausgegangen, sondern von den notwendigen Anforderungen und Eingangsgrößen, welche für die Cyber-Resilienz-Metriken relevant sind. Es wird die prinzipielle Machbarkeit des gewählten Ansatzes aufgezeigt. Weitere Evaluierungszyklen im Sinne des DSR sind notwendig. In einem ersten Schritt werden Metriken für die Cyber-Resilienz analysiert. Basierend auf deren Eigenschaften und notwendigen Eingabewerten können die Mindestanforderungen an ein Modell für die Emulation definiert werden. Diese Anforderungen gilt es anschließend aufzuarbeiten und hinsichtlich ihrer Umsetzbarkeit zu prüfen.

Nicht mehr Bestandteil dieses Beitrags ist die Evaluierung des Ansatzes hinsichtlich seiner Eignung und Aussagekraft bezüglich der Problemstellung. Wird das Problem nicht ausreichend adressiert, fließen die daraus resultierenden Anpassungen wieder in das Design des Modells sowie eine erneute Evaluierung ein.

## 3. Ergebnisse

*Analyse der Cyber-Resilienz-Metriken*

Grundsätzlich kann jede Cyber-Metrik, die sich auf die Ziele Antizipieren, Widerstehen, Wiederherstellen und Anpassen[2] (Bodeau et al., 2018b) bezieht, als Cyber-Resilienz-Metrik verwendet werden. Auch Metriken, die keinen direkten Zusammenhang zur Resilienz aufweisen, sondern auf grundlegende Merkmale wie Ausfallsicherheit und Verfügbarkeit referenzieren, können für die Resilienzmessung eingesetzt werden (Kott et al., 2018). In ENISA (2011) werden 24 grundlegende Metriken[3] zur Widerstandsfähigkeit von netzwerkbasierten Diensten vorgestellt. Bodeau et al. (2018a) enthält einen Katalog mit fast 500 repräsentativen Cyber-Resilienz-Metriken. Domänenspezifisch führen Vugrin et al. (2017) beispielhaft 20 Resilienzmetriken für Energienetze auf und Kerkdijk et al. (2017) orientieren sich an der Cyber-Kill-Chain, analysiert 23 Angriffsszenarien auf den Finanzsektor und leitet daraus 47 Cyber-Resilienz-Metriken ab. Eine Analyse dieser Metriken führt zu folgenden Erkenntnissen:

- Grundlegend werden die Eigenschaften der technischen Infrastruktur (z. B. Anzahl, Verfügbarkeit, Konfiguration) und der organisatorischen Prozesse (z. B. Personal, Verhalten, Abläufe, Dauer) messbar gemacht. Diese beiden Bereiche gilt es zu emulieren.

- Da eine Vielzahl von allgemeinen sowie domänenspezifischen Cyber-Resilienz-Metriken existiert, ist eine Einbeziehung aller dieser Metriken sehr komplex und nicht trivial.

- Als Eingabewerte für die Metriken werden geeignete Messwerte benötigt. Ohne diese können die Metriken nicht verwendet werden bzw. liefern keine Ergebnisse. Die meisten Metriken basieren auf Cybereereignissen, deren Eintreten in der Praxis nicht direkt kontrolliert werden kann. Dieser Umstand führt folglich zu langen Mess- und Beobachtungszeiträumen. Relevant für die Messwerte bzw. als Datengrundlage ist meistens auch nicht das Ereignis an sich, sondern dessen Auswirkung.

- Alexeev et al. (2017) unterscheiden zwischen struktureller und aktiver (reaktiver und adaptiver) Resilienz. Ein ähnlicher, aber passenderer Ansatz ist die Unterteilung in ereignisbasierte (event-based) und ereignisunabhängige (non-event-

[2] *anticipate, withstand, recover and adapt*
[3] *baseline resilience metrics*

based) Cyber-Resilienz-Metriken. Ereignisunabhängige Metriken beziehen sich auf präventive Maßnahmen bzw. auf das Ziel der Antizipation.

- Es werden keine Anforderungen an die Quantität oder die Qualität der ihnen zugrundliegenden Messwerte definiert. Beide Größen haben allerdings direkte Auswirkungen auf die Aussagekraft der Metriken.
- Es werden keine konkreten Zielwerte definiert (z. B. 80 Prozent als Mindestwert oder zwei Stunden als Zeitfenster für eine Reaktion auf ein Ereignis), die es zu erreichen gilt.

Alle Kriterien oder Anforderungen, die nicht von den Cyber-Resilienz-Metriken spezifiziert werden, sind für die Vorhersage der Cyber-Resilienz auf Basis dieser Metriken nicht relevant und werden daher nicht weiter betrachtet.

*Anforderungen an die Emulation*

Das Ziel ist die Vorhersage der Cyber-Resilienz einer Organisation. Folgende Anforderungen an ein dafür geeignetes Emulationsmodell sind mindestens zu erfüllen:

- Anwendung einer Vielzahl an verschiedenen Cyber-Resilienz-Metriken
- Darstellung des Auftretens von Cyberereignissen über verschiedene Zeiträume
- Abbildung der technischen Infrastruktur und der organisatorischen Prozesse einer Organisation

Für den Einsatz einer Vielzahl von Cyber-Resilienz-Metriken sind die benötigten Eingabewerte bzw. Messwerte zur Verfügung zu stellen. Dazu gehören mindestens folgende abstrahierte Eigenschaften:

- Art und Häufigkeit des Auftretens eines Ereignisses über einen bestimmten Zeitraum
- Dauer für einen (organisatorischen) Prozess und beteiligte Akteure
- Anzahl an Komponenten/Systemen/Ressourcen und deren verschiedene Zustände
  (z. B. System *x* redundant ausgelegt, Verfügbarkeit, Echtzeitfähigkeit)
- notwendige Eigenschaften und Schwellenwerte für die Aufrechterhaltung der Zustände (z. B. maximale Anzahl an Anfragen, max. 4ms Latenz für Echtzeitfähigkeit)
- zeitliches Verhaltensmuster einer Komponente, eines Systems oder einer Ressource (z. B. Änderung des Zustandes)
- Eigenschaften der technischen und organisatorischen Kommunikationswege (z. B. Bandbreite, Latenz bzw. Laufzeiten)

Für ereignisunabhängige Metriken ist eine Vorhersage trivial, sie basiert auf statischen Gegebenheiten der technischen Infrastruktur sowie der organisatorischen Prozesse. Im Gegensatz dazu werden für ereignisbasierte Metriken Messwerte benötigt, die vom Auftreten von Cyberereignissen abhängig sind. Ein solches Ereignis wird in erster Linie

durch seine Auswirkungen auf ein System beschrieben und kann wie folgt dargestellt werden:

- Art und Häufigkeit des Auftretens über einen bestimmten Zeitraum
- Auswirkung auf die Dauer eines (organisatorischen) Prozesses und die beteiligten Akteure
- Auswirkung auf den Zustand einer Komponente, eines Systems oder Ressource
- Auswirkung auf die Eigenschaften einer Komponente, eines Systems, einer Ressource oder der technischen und organisatorischen Kommunikationswege

Für die Modellierung von Geschäftsprozessen wird die *Business Process Model and Notation* (BMPN) verwendet. Sie ist standardisiert, weit verbreitet und kann leicht automatisiert werden. Im Idealfall sind die Geschäftsprozesse einer Organisation bereits in BPMN modelliert.

Für die Darstellung der technischen Infrastruktur ist es nicht erforderlich, die tatsächliche Komplexität einer Komponente oder eines Systems abzubilden. Es ist ausreichend, die Auswirkung eines Ereignisses darzustellen. Dies geschieht durch Emulation des Laufzeitverhaltens einer Komponente bzw. eines Systems. Für die Modellierung der technischen Infrastruktur wird Emulab eingesetzt.

**4. Auswertung und Zusammenfassung**

Durch die Analyse verschiedener Cyber-Resilienz-Metriken konnten grundlegende Erkenntnisse bezüglich der Voraussetzungen für eine Emulation ermittelt werden. Darauf aufbauend wurden Anforderungen an ein Emulationsmodell erarbeitet. Prinzipiell ergeben sich drei Herausforderungen für eine Emulation:

- Es gibt eine Vielzahl von Cyber-Resilienz-Metriken, die mit den notwendigen Eingabewerten versorgt werden müssen.
- Verschiedene unterschiedliche Cyberereignisse müssen darstellbar sein.
- Die Abbildung der technischen Infrastruktur sowie von Geschäftsprozessen muss möglich sein.

Für den Einsatz der Metriken wurden sechs Mindestanforderungen für die Bereitstellung der Eingabewerte definiert. Diese müssen vom Emulationsmodell zur Verfügung gestellt werden. Die Umsetzung dieser Kriterien wird als realisierbar bewertet. Für die Abbildung von Cyberereignissen wurden vier grundlegende Auswirkungen auf die Eigenschaften des Modells erarbeitet. Für die Modellierung der Geschäftsprozesse mit der *Business Process Model and Notation* (BMPN) sowie der technischen Infrastruktur basierend auf Emulab wurden etablierte und erweiterbare Ansätze gewählt.

Die aufgestellte Hypothese kann auf folgende Fragestellung reduziert werden: Können die notwendigen Daten (Messwerte) für die Bewertung der Cyber-Resilienz mithilfe einer Emulation erzeugt werden? Diese Frage und damit auch die Hypothese kann vom konzeptionellen Standpunkt her positiv beantwortet werden.

*Einschränkungen*

Dieser Beitrag zeigt lediglich einen konzeptionellen Ansatz und lässt den Nachweis der Funktionsweise bzw. der konkreten Anwendbarkeit offen. Aufgrund des iterativen Vorgehensmodells kann noch nicht von einer abschließenden Betrachtung gesprochen werden.

## 5. Ausblick

Zur Optimierung des Ansatzes sind noch mehrere Evaluierungszyklen nach der Design Science Research Methodologie erforderlich. Daraus können sich noch zusätzliche Anforderungen an die Emulation ergeben. Essenziell ist die Evaluierung des konzeptionellen Ansatzes mit Beispielen aus der Praxis.

Eine Konkretisierung der sicherheitskritischen Ereignisse kann durch die Einbindung des MITRE ATT&CK Frameworks erfolgen.

Die Emulation der technischen Infrastruktur kann alternativ mit den Werkzeugen *GNS3 (Graphical Network Simulator-3)* oder *EVE-NG* erfolgen.

Für die Modellierung der Geschäftsprozesse kann anstelle der Modellierungssprache *Business Process Model and Notation* (BPMN) die Verwendung von *erweiterten Ereignisgesteuerten Prozessketten* (eEPK) in Betracht gezogen werden. Alternativ zur Emulation bzw. als möglicher nächster Schritt wäre eine Simulation der IT/OT-Infrastruktur denkbar. Damit würde man eine möglichst geringe Abstraktion und realitätsnahe Abbildung der Organisation erreichen.

Die Abbildung der Geschäftsprozesse kann um Geschäftsziele und spezifische Kennzahlen der Organisation erweitert werden, z. B. durch die Integration einer (Risiko) Balanced Scorecard. Der Ansatz kann zudem durch die Verwendung bestehender und bewährter Enterprise Architecture Frameworks wie z. B. TOGAF (The Open Group Architecture Framework) oder ArchiMate erweitert werden.

Darüber hinaus ist zu prüfen, inwieweit der gewählte Ansatz stärker mit bestehenden Cyber-Resilienz-Frameworks verknüpft bzw. erweitert werden kann. Beispielhaft seien hier das NIST Cyber Resilience Framework, NIST SP 800-160 "*Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*" (Ross et al., 2021) oder der Cyber Resilience Review (CRR) des Department of Homeland Security's Office of Cybersecurity & Communications genannt.

## Quellen

Alexeev, A., Henshel, D. S., Levitt, K., McDaniel, P., Rivera, B. K., Templeton, S. P. & Weisman, M. (2017). Constructing a Science of Cyber-Resilience for Military Systems. NATO IST-153/RWS-21 Workshop on Cyber Resilience, 30–42.

Bernardin, E. & Greiman, V. A. (2021). Cyber Resilience: A Global Challenge. ACPIL

Bodeau, D. J., Graubart, R. D., McQuaid R. M. & Woodill J. (2018a). Cyber Resiliency Metrics Catalog. MITRE Technical Report. https://www.mitre.org/sites/default/files/2021-11/pr-18-3376-cyber-resiliency-metrics-catalog.pdf

Bodeau, D. J., Graubart, R. D., McQuaid R. M. & Woodill J. (2018b). Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and

Program Managers to Select the Most Useful Assessment Methods. MITRE Technical Report. https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

ENISA. (2011). Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report. https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport

Kerkdijk, R., Lagarde, R., Koens, T., Zeijlemaker, S., Samwel, P., te Paske, B.-J., Verweij, E., & Wolthuis, R. (2017). Library of Cyber Resilience Metrics.

Kott, A., Blakely, B., Henshel, D. S., Wehner, G. J., Rowell, J., Evans, N. R., Muñoz-González, L., Leslie, N. O., French, D. A., Woodard, D. B., Krutilla, K., Joyce, A. W., Linkov, I., Machuca, C. M., Sztipanovits, J., Harney, H., Kergl, D., Nejib, P., Yakabovicz, E., . . . Møller, A. (2018). Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153. arXiv (Cornell University). https://apps.dtic.mil/dtic/tr/fulltext/u2/1050894.pdf

Lang, C. & Madahar, B. (2017). Understanding the mission impact of a cyber attack in a system of systems environment. NATO IST-156 Workshop on Modelling and Simulation.

Linkov, I., Eisenberg, D., Plourde, K. J., Seager, T. P., Allen, J. H. & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

Musman, S., Temin, A., Tanner, M., Fox, R. & Pridemore, B. (2013). Evaluating the impact of cyber attacks on missions. M&S Journal, 8(2), 25–35. https://www.mitre.org/sites/default/files/pdf/09_4577.pdf

Ross, R. S., Pillitteri, V., Graubart, R., Bodeau, D. & McQuaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Volume 2, Revision 1. https://doi.org/10.6028/nist.sp.800-160v2r1

Siaterlis, C., Perez-Garcia, A. & Masera, M. (2011). Using an Emulation Testbed for Operational Cyber Security Exercises. IFIP advances in information and communication technology, 185–199. https://doi.org/10.1007/978-3-642-24864-1_13

Siaterlis, C., García, A. J. & Genge, B. (2013). On the Use of Emulab Testbeds for Scientifically Rigorous Experiments. IEEE Communications Surveys and Tutorials, 15(2), 929–942. https://doi.org/10.1109/surv.2012.0601112.00185

Vugrin, E. D., Castillo, A. & Silva-Monroy, C. A. (2017). Resilience Metrics for the Electric Power System: A Performance-Based Approach. OSTI OAI (U.S. Department of Energy Office of Scientific and Technical Information). https://doi.org/10.2172/1367499