
PARANOR
The Digital
Business
Developers
Safety.
Relevant.
Software.
Report No 1

Inhalt

Editorial No 1

Sicherheitsrelevante Software

Dr. Stéphane Barbey
Mitglied der Geschäftsleitung

Liebe Leser, liebe Leserinnen

«Grundlegender Software-Fehler in der Boeing 737 Max gefunden», titelte die NZZ am 5. August 2019. Dieser Erkenntnis gingen zwei Abstürze von Flugzeugen des Typs Boeing 737 Max innerhalb eines knappen halben Jahres mit insgesamt 346 Toten voraus.

Wir alle wissen es längst – Software ist in jedem Bereich unseres Lebens angekommen und übernimmt in vielen Fällen Funktionen, die von Menschenhand nicht mehr ausgeführt werden können. Oftmals handelt es sich hierbei um Funktionen, die bei Fehlverhalten der Software schwere Schäden oder gar Todesfälle zur Folge haben.

Im Fall der Boeing 737 Max waren die Abstürze wohl nicht auf einen einzelnen Software-Fehler zurückzuführen. Vielmehr war es ein Zusammenspiel von Hardware, Software und System-Design. Statt beide Bordcomputer gleichzeitig zu verwenden und sich gegenseitig kontrollieren zu lassen, wurden die Rechner abwechselnd genutzt. Nur einer von zwei verfügbaren Sensoren für den Anstellwinkel wurde ausgelesen und ein Fehler im Mikroprozessor eines Bordcomputers wurde entdeckt. Zudem griff die Software des automatischen Trimmsystems bei Fehlverhalten in einer für den Piloten nicht beherrschbaren Art und Weise in die Flugsteuerung ein.

Obwohl solche sicherheitsgerichteten Systeme immer ganzheitlich zu betrachten sind, erlauben wir uns als Software-Entwicklungsfirma, uns auf die Software-Aspekte zu konzentrieren.

Mit diesem Report halten Sie, liebe Leserinnen und Leser, die erste Ausgabe einer neuen Serie von gesammelten White Papers in Ihren Händen. Wir möchten Sie fortan in losen Abständen mit fundierten Informationen zu Themen versorgen, die wir als wichtig erachten. Hierfür lassen wir ausgewählte Partner, Vertreter von Forschung, Entwicklung und Bildungsinstitutionen sowie Angestellte von Paranor zu Wort kommen.

Report No. 1 widmet sich dem Thema sicherheitsgerichtete Software und beleuchtet in drei White Papers, wie sich die Zuverlässigkeit von Software vorhersagen lässt, worauf bei der Gestaltung der Mensch-Maschine-Interaktion Wert gelegt werden sollte und welche Skills und Kompetenzen erforderlich sind, um sicherheitsgerichtete Systeme bauen zu können.

Wir möchten uns an dieser Stelle ganz herzlich bei unseren vier Gastautoren Dr. Ossmane Krini, Dr. Christian Reuter, Dr. Simon Moser und Fridel Rickenbacher bedanken.

Ich wünsche Ihnen viel Spass bei der Lektüre!

03 Skills und Kompetenzen bei Entwicklung und Betrieb sicherheits-relevanter IT-Systeme zugunsten der Cyber-Resilienz

Dr. Simon Moser
FSIE, Förderverein Schweizer Informatikexpertinnen und -experten, Bern, www.fsie.ch

M.Sc. Fridel Rickenbacher
FSIE Fachkommission Security & Quality, Förderverein Schweizer Informatikexpertinnen und -experten, Bern, www.fsie.ch
Senior Consultant, eXecure AG, Swiss IT Security Group, www.execure.ch

1
Digitale Skills und «digitale Mündigkeit» für alle, aber nicht für alles

Die Digitalisierung von Prozessen in allen Branchen und in der Verwaltung schreitet mit grosser Dynamik voran. Es entstehen laufend neue Möglichkeiten, neue Prozesse, neue Abhängigkeiten, neue Risiken. Altes wird obsolet und der dynamische «Stand der Technik» immer relevanter und herausfordernder.

Dies führte und führt zur Forderung, dass bereits in der Grundschule nicht nur IT-Anwenderwissen vermittelt werden soll. Auch sogenannte «Computational Skills» – das Verstehen und gar Entwickeln von Algorithmen und Datenstrukturen – sollen in den obligatorischen und sekundären Schulen im Lehrplan integriert werden. Das finden wir unterstützenswert und relevant für eine möglichst gute «digitale Mündigkeit» im Zeitalter der anzustrebenden «Cyber-Souveränität».

Aber ist es das Ziel, dass alle Grundschulabsolvierenden bei der Planung, Entwicklung und dem Betrieb von IT-gestützten Prozessen Entscheide vorbereiten, fällen und umsetzen sollen?

Die Frage kann man mit einer Analogie aus dem medizinischen Bereich analysieren: Ist jeder mit dem Grundschulwissen über den menschlichen Körper, mögliche Krankheitsbilder und Behandlungsmethoden befähigt, medizinische Diagnosen und Behandlungen durchzuführen? Hier lautet die Antwort klar: Nein. Aber alle sollen in Trivialfällen wie Schnupfen oder Grippe sich selbst helfen können und – besonders wichtig – genügend Wissen haben, um im Rahmen eines Grundverständnisses zwischen Trivialfällen und ernsthafteren Symptomen unterscheiden zu können.

Zurück in die IT-Welt: Wenn wir eine sichere und verlässliche IT-Infrastruktur wollen, dann müssen wir vermutlich auch hier die nicht-trivialen Arbeiten den gut ausgebildeten oder höher spezialisierten Experten überlassen, Profis mit grösseren methodischen und Best-Practice-basierten Erfahrungen. Also muss die eingangs gestellte Frage auch mit Nein beantwortet werden.

Es ergeben sich aber damit sofort Folgefragen: Wie kann in Digitalisierungsfragen zwischen trivial und nicht-trivial unterschieden werden? Hat die Schweiz ein ausreichendes Bildungs- und vor allem auch Weiter- und Fortbildungssystem für IT-Experten?

Darauf wollen wir im vorliegenden Bericht eingehen.

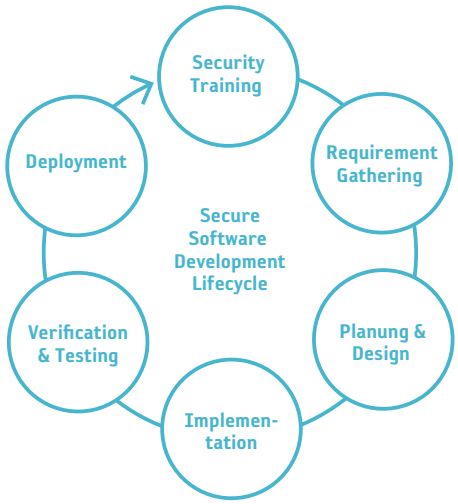
2
Herausforderungen im Kontext sicherheitsrelevanter und systemkritischer IT-Systeme

Bei der Projektierung
Hier besteht die Herausforderung darin, bei projektierten neuen digitalisierten Prozessen, Anpassungen, Secure Coding, Cyber Security und/oder Phase-outs überhaupt zu erkennen, dass es sich um nicht-triviale Fälle handelt. Eine besondere Herausforderung ist es zusätzlich, zu wissen, dass selbst triviale Anpassungen, also auch solche, die ein Anwender oder Administrator mit simplen Eingaben oder Konfigurationsänderungen bewirken kann, die dynamische Sicherheitssituation bezüglich Angriffs- und Betriebssicherheit von Systemen grundlegend verändern können.

Also wissen wir nun: Trivial und sicherheitsrelevant ist nicht dasselbe. Doch was tun wir mit dieser Erkenntnis? Und wie steht es mit den direkten und insbesondere indirekten Auswirkungen einer projektierten Anpassung auf andere Prozesse, mit der mehrschichtigen Gesamtsicherheit und der Sicherheitsstrategie? Zudem: Kann auch – bei unverändertem IT-System — dessen neue oder geänderte Art/Konvention der Anwendung oder gar nur die Änderung eines Nicht-IT-Prozesses Auswirkungen auf die Gesamtsystem-Sicherheit haben?

Es braucht Erfahrung und Skills sowie professionell dokumentierte und modellierte Systeme – zum Beispiel nach den State-of-the-art-Konventionen mit BPMN, Security Development Lifecycle (SDL) oder UML erarbeitete Abhängigkeitsnetzwerke –, um bei Projekten systematisch analysieren zu können, ob sich mit dem «Ziehen an einem Faden» ganze andere Systemteile mitbewegen oder nicht. In einer mehrschichtigen Gesamtsicherheits-Architektur und deren umfassenden ICT-Strategie müssen solche Themen, Schnittstellen und Komponenten prozessual und technisch im Rahmen von wiederkehrenden Audits und den grundsätzlichen Compliance-Anforderungen überwacht, überprüft und bei Bedarf angepasst werden.

Sobald sich also ein IT-System ausserhalb einfacher Privat-Websites, statischer Websites, Web-Shops, Blogs, Games, Apps, Microservices, API etc. in Richtung eines systemrelevanten oder gar systemkritischen Systems bewegt, plädieren wir dafür, bei allen Projekten – selbst bei einfacheren Business-Projekten – schon in den frühen Analysephasen einen IT-Experten oder IT-Berater mit den entsprechenden Kompetenzen (methodisch, BPMN/UML, fachliches Branchenwissen) hinzuzuziehen. Der Experte gewährleistet die Beurteilung der Kritikalität, das IT-Riskmanagement und liefert eine Zweitmeinung bezüglich Sicherheit sowie anderen Auswirkungen, insbesondere auf die Qualität und Inter-Prozess-Abhängigkeiten. Ein einfaches Anschauungsbeispiel: Vermeintlich triviale Produkteinführungen und/oder Anpassungen, etwa bei der Spedition oder bei Produktions-/Maschinen-Steuerungen, können massive Auswirkungen auf Wartezeiten oder Unterbruchszeiten zur Folge haben, die wiederum weitere Auswirkungen mit sich bringen – bis hin zu vertragsrelevanten Folgen mit finanziellen Implikationen oder gar Haftungsfragen.



Bei der Umsetzung
Trustworthy Computing Security Development Lifecycle (Abgekürzt SDL, zu Deutsch Entwicklungszyklus für vertrauenswürdigen Computereinsatz) ist ein 2004 von Microsoft veröffentlichtes Konzept

zur Entwicklung von sicherer Software und richtet sich an Software-Entwickler, die Lösungen anbieten, die böswilligen Angriffen standhalten müssen. Stark vereinfacht handelt es sich dabei um Gebote und Verbote, Tipps und Tools.

Der SDL besteht aus einer Vielzahl von Komponenten, die den kompletten Entwicklungszyklus eines Software-Produkts begleiten. Im Prinzip ist der SDL eine umfangreiche und von Produkt zu Produkt variierende Checkliste. Diese Liste kann mehr als 700 Punkte lang sein und muss von den Entwicklern vollständig abgearbeitet werden, bevor ein Software-Produkt freigegeben wird.

So schreibt der SDL zum Beispiel bestimmte Einstellungen beim Kompilieren oder spezielle Kommandos vor. Ausserdem umfasst er Richtlinien, wie und womit der Quellcode auf Schwachstellen getestet werden muss. Der SLD fordert jeden Entwickler dazu auf, sich Gedanken über mögliche Angriffe auf seinen Code zu machen (Threat Modelling) und versucht so, die angreifbaren Stellen zu minimieren: Nicht dringend benötigte Funktionen sind im Lieferzustand der Programme abgeschaltet, um mögliche Einfallstore für Cyber Crime zu minimieren.

Ein weiteres Konzept fügt das IT-Security-Team (Sec) mit dem IT-Betrieb (Ops) sowie dem Entwicklungsteam (Dev) zusammen. Da alle drei Teams zusammenarbeiten, ist es einfacher, Sicherheitskontrollen in die Implementierungs-Pipeline zu integrieren, was Verzögerungen und Probleme reduziert, die entstehen, wenn ein Unternehmen die Security vom Entwicklungsprozess trennt. Und mit der Automatisierung, die durch Cloud Computing möglich ist, können Unternehmen mit weniger Verzögerungen und Ausfallzeiten aufgrund von Sicherheitsmängeln effizienter werden.

Kurzfristige und marktorientierte Optimierungen stellen sich ansonsten trotz der hohen Dynamik des «Stands der Technik» schnell als schädlich heraus, gerade angesichts der sehr dynamischen Bedrohungslage in den Bereichen Cyber Security, Cyber Crime und Cyber-Resilienz.

Daraus ergeben sich gewisse Fragestellungen und Herausforderungen:

- Testvorbereitungen und Testzeiten (unter dem Druck von Markteinführungen)
- Testumgebungen (Existieren realistische Situationen? Steht genügend Masse an Prozessen und Daten zur Verfügung? Ist die Konfigurationsgleichheit von Test- und Produktionsumgebungen sichergestellt?)
- Sicherheit und deren Voreinstellungen (z. B. security by design, security by default, Datenminimierung, Datenanonymisierung) stehen über allem – auch über der Usability und User Experience?

Im Betrieb

Essenziell sind eine kontinuierliche Überwachung, Incidents und Near Incidents Reporting, Incidents Prediction und Prevention (Data Science), Interventions sowie «SIEM Security Information and Event Management». Bei erweiterten Anforderungen aus Sicht der IT (Information Technology) und OT (Operation Technology) können mitunter auch «Security Operation Center / SOC as a service» mit automatisierten ersten Gegenmassnahmen oder Schadensminderungen unumgänglich sein, gerade im Zeitalter von maximaler Systemabhängigkeit und Cyber Crime. Ein dynamisch-proaktives IT-Riskmanagement sollte auf die hohe Dynamik des «Stands der Technik» und auf Marktanforderungen reagieren und kann mittels entsprechender Experten (z.B. DevSecOps) und Audits optimiert werden.

Im Rahmen einer neuen Kultur des proaktiven Know-how-Managements und -Transfers können solche Use Cases und bewährte Best-Practice-Beispiele mittels «Lessons Learned Sessions» in Erfahrungsaustausch-Gruppen methodisch und agil in der internen Organisation oder gar Partnerorganisation gelebt und gehaltvoll genutzt werden.

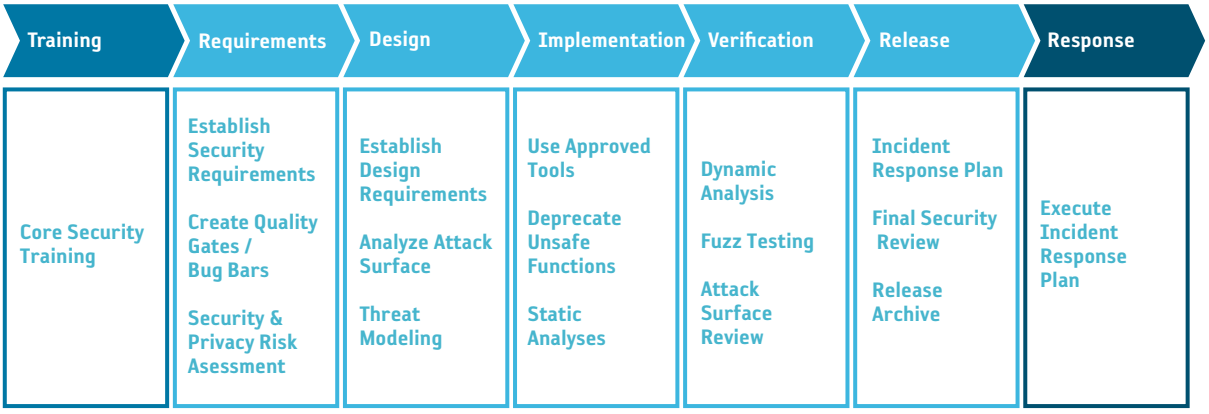


Abbildung: Security Development Lifecycle (SDL)

3
Skills und Kompetenzen auf dem neuesten Stand – IT-Experten FSIE™ Security

Die in Kapitel 2 skizzierten Herausforderungen legen nahe, dass nur auf dem aktuellen «Stand der Technik» ausgebildete und praxiserfahrene Experten diese in realen Situationen unterstützen, optimieren und meistern können. Wie findet man diese in der Schweiz?

Das Schweizer Bildungssystem stellt für IT-Berufsleute eine gute und vielfältige Basis-Bildungslandschaft zur Verfügung: Berufsbildung (ca. 1500 EFZ-Abschlüsse pro Jahr), Höhere Fachschule (ca. 1000 Abschlüsse pro Jahr), Bachelor (ca. 800 Abschlüsse pro Jahr), Master (ca. 500 Abschlüsse pro Jahr), Ph.D. (ca. 150 Abschlüsse pro Jahr). Aber bei der Weiterbildung zum Spezialisten, zum Beispiel für Cyber Security oder Security DevOps (DevSecOps), und insbesondere bei der Fortbildung, sprich der laufenden Aktualisierung oder gar Rezertifizierung des erworbenen Wissens, gibt es zurzeit keine einheitliche Systematik aller Akteure und Organisationen.

Hier schafft der 2017 neu gegründete Verband FSIE (Förderverein Schweizer Informatikexpertinnen und -experten), der im Rahmen von ICTswitzerland (www.ictswitzerland.ch) organisiert ist, Abhilfe: Er definiert für aktuell fünf Spezialisierungen – Engineering, Security, BRIDGE (Projektmanagement und Business Analyse kombiniert), User Experience und Quality – ein strukturiertes Weiter- und Fortbildungsschema mit dem Fachtitel Experte FSIE™.

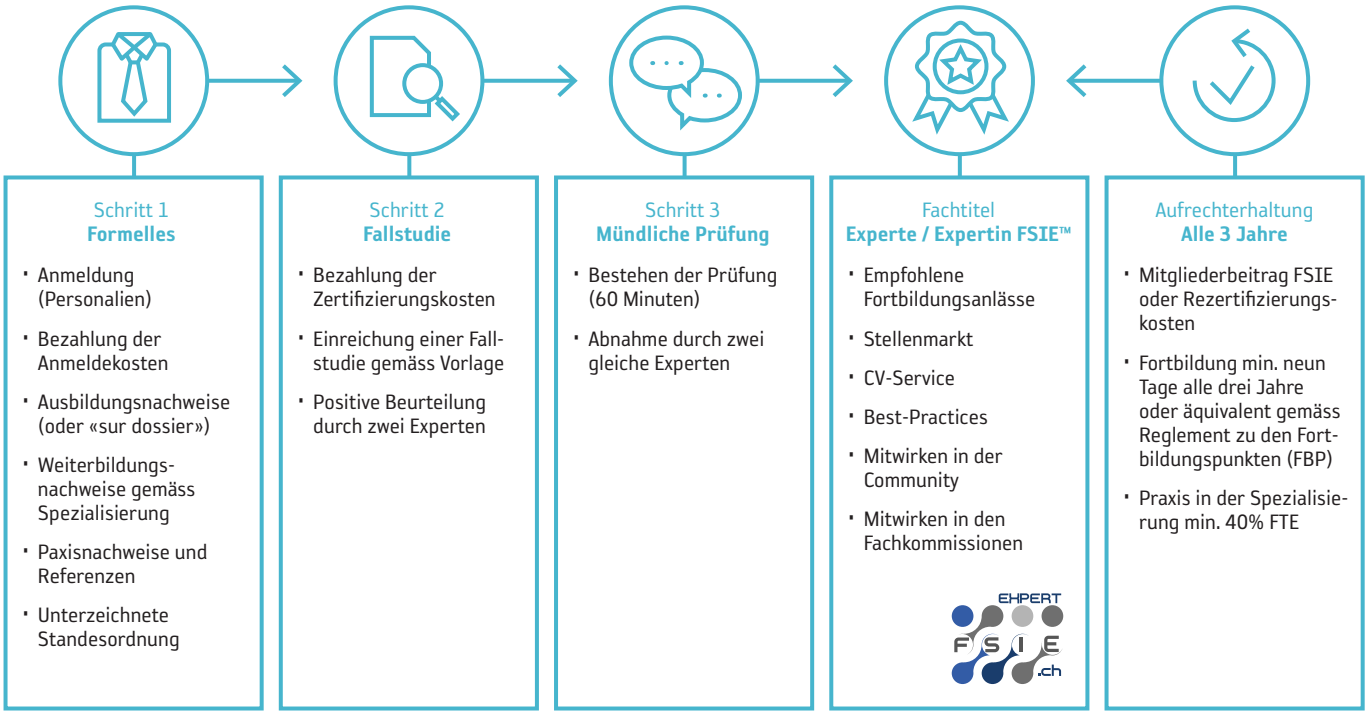


Abbildung:
Schema zur Erlangung und Aufrechterhaltung des Titels Experte FSIE™

4
Fazit

Sichere Systeme beziehungsweise möglichst abgesicherte Systeme und Software sollten möglichst auf den dynamischen «Stand der Technik» ausgerichtet werden.

Diese neue Selbstverständlichkeit verlangt von allen Akteuren auf einer strategischen und methodischen, interdisziplinären Ebene einen gemeinsamen Konsens und gar eine neue Selbstverständlichkeit – ausserhalb einer Überregulierung. Usable Safety Engineering umfasst die gebrauchstaugliche Gestaltung interaktiver und kooperativer sicherheitskritischer Systeme. Neben der Anwendung von in der MCI bekannten Methoden oder Security Development Lifecycle (SDL) sind einige Besonderheiten zu berücksichtigen:

- **Secure by design**
  Schon in der Planungsphase sollte auf die Sicherheitsbelange der Software eingegangen werden.
- **Secure by default**
  Trotz sorgfältigster Planung sollte ein Entwickler vom Vorhandensein von Sicherheitslücken ausgehen. Aus diesem Grund sollten die Standardeinstellungen (z. B. erforderliche Privilegien) möglichst niedrig gewählt werden und selten benutzte Features standardmässig deaktiviert werden.
- **Secure in deployment**
  Die mitgelieferten Dokumentationen und Tools sollen die Administratoren dabei unterstützen, die Software möglichst optimal einzurichten.
- **Communications (Software)**
  Die Entwickler sollten offen mit möglichen Sicherheitslücken umgehen und den Endanwendern schnell Patches oder Workarounds zur Verfügung stellen.
- **Privacy by design**
  Schon in der Planungsphase sollten Datenschutzbelange der Software berücksichtigt werden.
- **Privacy by default**
  Die Standardeinstellungen der Software sollten konservativ gewählt werden.
- **Privacy in deployment**
  Datenschutzmechanismen sollten offengelegt werden, um es Administratoren zu ermöglichen, die internen Datenschutzrichtlinien des Unternehmens umzusetzen.
- **Communications (Privacy)**
  Datenschutzerklärungen sollten transparent formuliert werden. Ein Team für Datenschutzvorfälle sollte eingerichtet werden.

Latente und aktive menschliche Fehler können in einer Verkettung von unglücklichen Ereignissen und Unfallursachen zum Zusammenbruch oder zur Kompromittierung von komplexen oder systemkritischen Systemen führen. Mittels entsprechender methodischer, prozessualer und technischer Massnahmen muss hier massgeschneidert orchestriert entgegengewirkt werden – auf den Ebenen Entwicklung, Umsetzung, Betrieb und Weiterentwicklung des Gesamtsystems.

Die Sensibilisierung der zunehmend angegriffenen «Schwachstelle» Mensch mit dessen Identität und personenbezogenen Daten ist ein wichtiger Faktor beim Erreichen eines möglichst hohen Gesamtsicherheits-Niveaus.

Dass unverändert und zunehmend der Mensch und dessen Identität und Rechte das wichtigste Angriffsziel bleiben, zeigen die folgenden einfachen Statistik-Aussagen: Rund 90 Prozent der erfolgreichen Attacken starten mit einer Phishing-Mail, das auf Social Engineering basiert, dem geschickt manipulierten Ausnutzen der menschlichen Tendenz zu Gutgläubigkeit und Vertrauen. Danach entsteht bei rund 80 Prozent der Fälle ein weitergehender Schaden wegen zu schwacher Kennwörter und Systemschutz oder zu hoher Berechtigungen des angegriffenen Mitarbeiters in der angezielten Systemumgebung.

Der Mensch als kritisches Einfallstor für Cyber-Attacken muss umfassend informiert, aufgeklärt, unterstützt und geschützt werden, damit er überhaupt eine persönliche Mitverantwortung tragen kann.

Die Technik alleine reicht nicht mehr gegen die dynamischen Bedrohungslagen von Cyber Crime, gegen immer ausgereiftere Phishing-Mails, Phishing-Webseiten und Social Engineering Attacken. Der weltweit sprunghaft ansteigende Wirtschaftsfaktor Cyber Crime bedient sich zudem schier unerschöpflicher monetärer und technologischer Ressourcen und nutzt auch die andere, die «dunkle Seite der Macht» (Dual-Use-Problematik) von neuesten technologischen Errungenschaften rund um Künstliche Intelligenz (KI/AI) oder Super High Computing.

Die Sicherheitsfrage lässt sich nicht auf Knopfdruck oder mittels nur eines Systems lösen. Auch gibt es keine Universallösung für alle Sicherheitsprobleme in der Vision von Security Automation. Die umfassende Verteidigung bei einem Angriff, der darauf abzielt, unberechtigten Zugriff auf personen- oder firmensensitive Informationen zu erlangen, sollte mittels einer mehrschichtigen Sicherheit und Ausrichtung auf Security Automation und Security Development Lifecycle (SDL) in der nötigen Tiefe und Ganzheitlichkeit erfolgen. Sinnvoll ist eine Strategie, bei der das Ausmass eines Angriffs und das Schadenspotenzial mithilfe zahlreicher Mechanismen und mehrerer Schutzebenen wirkungsvoll gedämpft oder entschleunigt werden.

Literatur und Quellen

1. Storey, N.: Safety Critical Computer Systems. Addison Wesley, Harlow, UK (1996)
2. Hoyos, C. (1990).: Menschliches Handeln in technischen Systemen. In: Hoyos, C. and Zimolong, B. (eds.) Ingenieurpsychologie. Enzyklopädie der Psychologie, Band 2,. pp. 1–30. Hogrefe, Göttingen
3. https://fridelonroad.wordpress.com/2019/06/20/swissict-resilienz-und-cyber-risikominimierung/
4. https://fridelonroad.wordpress.com/2019/01/16/digitalisierung-%c2%a6-cybersecurity-sensibilisierung-mehrschichtige-sicherheitsstrategie/
5. https://fridelonroad.wordpress.com/2018/06/22/cybersecurity-sensibilisierung-und-staerkung-der-schwachstelle-mensch-zugunsten-der-gesamtsicherheit/
6. https://fridelonroad.files.wordpress.com/2018/02/ksgv-ch-gewerbeverband-ausgabe-januar-2017-fridels_blog_fr.pdf
7. https://fridelonroad.wordpress.com/2018/03/11/security-by-design-in-massive-interconnected-systems-bim-smartcity-iot-ehealth/
8. https://fridelonroad.wordpress.com/2014/10/09/99-sicherheit-mensch-prozesse-technologie-risk-management/
9. https://fridelonroad.wordpress.com/2019/06/08/digitalisierung-cybersecurity-sensibilisierung-unbewusst-inkompetent-bei-cybersecurity/
10. https://fridelonroad.wordpress.com/2019/11/16/digitalisierung-cybersecurityresilienz-sensibilisierung-von-der-reaktion-zur-praevention-und-kampagnen-in-ict-prozessen-und-ict-budget-v2/
11. https://fridelonroad.wordpress.com/2019/10/19/digitalisierung-cybersecurityresilienz-sensibilisierung-ein-trainierter-guter-plan-und-human-cyber-resilience-firewall-fuer-bessere-cyberresilienz/

PARANOR
The Digital
Business
Developers

DACHCOM

Paranor AG
Juraweg 14
3046 Wahlendorf
Switzerland

Paranor Engineering AG
Achereggstrasse 7
6362 Stansstad
Switzerland

+41 31 828 92 22
info@paranor.ch
www.paranor.ch