IT-Sicherheitsmanagement – Zeit für einen Paradigmenwechsel

Frank W. Holliday, 17. Oktober 2017

Bei zunehmender Komplexität (Vielfalt/ multifacetiert/ mehrschichtig) + höherer Dynamik (zunehmender Veränderungsgeschwindigkeit) unserer IT- Landschaften und zunehmender Bedeutung für die Gestaltung und Abläufe unserer Lebensführung (Stichwort: Digitale Gesellschaft) wird das Ziel unser Leben auf der Basis sicherer Informationstechnologie zu führen für unsere moderne, komplexe Zivilisation zur Überlebensfrage. Bisherige Ansätze des IT-Sicherheitsmanagements, die auf dem bisherigen klassischen IT- Risikomanagement fußen, zeigen in Praxis erhebliche Unzulänglichkeiten auf. Die mehr und mehr gelungenen Zero-Day-Attacken illustrieren dieses Übel nur allzu deutlich. Auch die zunehmende Zahl von "Überraschungen" (Krisen) trotz intensivem Risikomanagement und intensiver Modellierungen, z.B. im Finanzsektor, zeigen auf, wir haben mit unseren bisherigen Ansätzen nur begrenzten Erfolg.

Woran liegt das?

Der bewusste Umgang mit Risiken (nichts anderes ist Risikomanagement) ist der Umgang mit Ungewissem. Wir wollen auf Überraschungen der Zukunft wenigstens vorbereitet sein. Nach unserem bisherigen physikalischen Weltverständnis ist die Welt auf dem Fundament der Quantenphysik aufgebaut, was bedeutet, die Zukunft dieser Welt ist naturgesetzlich nicht genau berechenbar (nicht-deterministisch) oder anders ausgedrückt erheblich zufällig. Gleichwohl versuchen wir Risiken zu taxieren, in Modellen zu verrechnen und damit auf die Zukunft besser vorbereitet zu sein. Gängige Vorgehensweise im IT-Risikomanagement ist hierzu möglichst umfassend in Szenarien Gefährdungen und Bedrohungen der Sicherheit zu erfassen, im Falle von Bedrohungen gilt es noch nach möglichen korrespondierenden Schwachstellen zu forschen, die erst eine Gefährdung auslösen. Ferner ist die Schutzbedürftigkeit gefährdeter Vermögenswerte (Kritikalität) festzustellen und daraus das sich ergebende Schadenspotential in der Regel als Produkt aus Schutzbedürftigkeit, Schadensvolumen und Eintrittswahrscheinlichkeit zu berechnen. Dieses dann nach den erfassten Szenarien aufgefächerte Schadenspotential-Profil wird dann nach zweckmäßigen Priorisierungen als berechnete strategische Grundlage für das Management von erforderlichen Gegenmaßnahmen herangezogen.

Nur reicht das?

Erstens sind wir für einen Erfolg bei dieser Vorgehensweise von einem möglichst sinnvoll getroffenen Umfang an erkannten Szenarien abhängig, das Spiel können wir schon allein vom Aufwand her nicht beliebig treiben. Doch birgt die Wahl der Sinn- und Abbruchkriterien für dieses Spiel große Brisanz [1] (Fukushima-Reaktoren-Katastrophe 2011: Flutwellen über 10 m Höhe wurden wegen der Einschätzung als Alle-vier-Jahrhunderte-Ereignis einfach im Szenarien-Katalog nicht mehr betrachtet. Die höchste gemessene Flutwelle im Küstengebiet betrug 23 m!). Zweitens haben wir aufgrund unseres relativ jungen Wissensgebiets IT-Sicherheit keine verlässlichen, noch wenig belastbare Häufigkeitsaussagen zu bestimmten Schadensereignissen, was auch dem Verbergen derselben (Gefahr eines Reputationsverlustes) geschuldet ist. Drittens führt es zum Phänomen, dass es, wenn

diese Vorgehensweise auch noch durch den Erhalt von Zertifikaten belohnt wird, zu einem Selbstläufer wird, dessen Wirksamkeit für die Realität an Rang verliert. Last but not least: da Sicherheit kein fixer Zustand ist, sondern aufgrund der technologischen Dynamik und des Unvorhergesehenen notwendigerweise einen kontinuierlichen Verbesserungsprozess darstellt, müssen wir dieses Spiel auch noch zyklisch betreiben um uns den Veränderungen der Welt wenigstens zu stellen. Die Gefahr ist groß, dass wir allein durch diesen betriebenen Aufwand unserer "modellierten Zukunft" übervertrauen.

Was tun?

Eine ähnliche Problemstellung haben wir beim Thema Gesundheit. An das Phänomen Gesundheit kann man aus dem Blickwinkel möglicher Krankheiten herangehen. Alle möglichen Fälle von Krankheiten werden erfasst, Therapien entwickelt und mehr und mehr nach ökonomischen Gesichtspunkten appliziert. Man kann das Phänomen Gesundheit aber auch aus der Sicht "gesund sein" (Salutogenese) betrachten. Der Erkenntnisgewinn ist dann ein ganz anderer. Nun kommen ganz andere Kategorien in den Fokus. Themen wie Robustheit, also die Fähigkeit gegenüber Belastungen standhalten zu können, und spezieller die Resilienz, die Fähigkeit Schocks und Störungen zu absorbieren und die Vitalität durch die Stresseinwirkungen für die Zukunft zu bewahren, kurz die Widerstandsfähigkeit, rücken in den Vordergrund.

Was bedeutet das übertragen auf unser IT-Sicherheitsmanagement?

Ein prinzipieller Systemsichtwechsel! Nur resiliente oder in der verfeinerten Begriffswelt als anti-fragil [2] gekennzeichnete Informationstechnologie-Systeme (und solche Systeme sind prinzipiell Menschen-Maschinen-Systeme) mit garantiert hoher Resilienz oder hohem Maß an Anti-Fragilität haben das Vertrauen verdient mit der erheblich zufälligen Zukunft umgehen zu können.

Was zeichnet diese Systeme aus?

Hierzu liefert die Natur reichliches Anschauungsmaterial. In der Natur ist ein großer Meta-Prozess zugange: die Evolution. Alle Phänomene der Natur ab Kategorie "Lebewesen" scheinen diesem Prozess Folge leisten zu müssen. Was zeichnet die Evolution aus? Zwei Konstruktionsprinzipien: Varianz und Selektion. Ein Mechanismus stellt Vielfalt her, ein weiterer Mechanismus sorgt dafür, dass nur die geschaffenen Varianten in Generationen weiterexistieren, die sich der Zukunft bewährt stellen, was "natürlich" ein hoch wechselwirkendes Prozessgeschehen darstellt. Sehr interessant ist hierbei, dass durch dieses hoch wechselwirkende Prozessgeschehen höchst kooperative Teilsysteme im System Natur zustande kommen, denn der Treiber ist nicht ein simples "survival of the fittest" im Sinne einer Dominanz gegenüber anderen Arten von Lebewesen, sondern der maßgebliche Treiber ist eine Maximierung symbiotischer Beziehungen – eines wechselseitigen Nutzens - unter den Arten!

Was sind die Kernelemente resilienter Systeme?

Interessanterweise im Wesentlichen zwei Komponenten: Zum einen Anpassungsfähigkeit, das Vermögen eines Systems, die nachteiligen Folgen von Veränderungen zu mindern und die Vorteile der Veränderungen zu nutzen (Systemlernfähigkeit). Zum anderen Bewältigungskapazität, das Vermögen vorhandene Ressourcen und Fähigkeiten zu nutzen um die Einwirkung von Schadensereignissen zu mindern und zu bewältigen (Systemerhaltungsreserve). Gerade ein Mangel an letzterer Komponente ist dafür verantwortlich, dass "effiziente Systeme" keinen nachhaltigen Erfolg garantieren, sie sind geradezu auf abspecken getrimmt, wehe sie werden krank bzw. passen nicht mehr zu den Umweltbedingungen. Zum Phänomen Resilienz lässt sich von Evolutionsbiologen interdisziplinär noch viel lernen.

Was zeichnet darüber hinaus anti-fragile Systeme aus?

Eine ausgeprägte Spezialität bei der Systemlernfähigkeit, die über die Anpassungsgeschwindigkeit der Evolution hinausgeht. Nämlich selbstorganisierend dafür zu sorgen aus erfolgten Belastungen der Robustheit für die zukünftige Ausgestaltung des Systems beschleunigt (nicht mehr über Generationsvariationen hinweg) adaptiv rückgekoppelt zu lernen (selbst lernend adaptierendes System – ein Prototyp davon ist der Mensch!).

Wenn es uns gelingt ein für die Sicherheit von Informationstechnologie-Systemen belastbares Maß für die System-Resilienz oder gar zur System-Anti-Fragilität abzuleiten, eröffnen sich für uns vollkommen neue Möglichkeiten mit Risiken umzugehen. Informationstechnologie-Systeme sind zu hohem Grade Artefakte und auch als solche modellier- oder wenigstens simulierbar. Dank unserer geschaffenen Möglichkeiten maschineller Informationsverarbeitung könnten wir nur solche Ausprägungen von Informationstechnologie-Systemen zulassen, die entweder evolutionär nach umfangreichen, schnellen, vielen Austestungen ein Mindestmaß an System-Resilienz unter Beweis gestellt haben oder durch Messbarkeit ein Mindestmaß an Anti-Fragilität als Systemeigenschaft besitzen. Zumindest wären das ganz neue Ansätze für eine Zertifizierung von sicheren Informationstechnologie-Systemen. Einen sehr interessanten Ansatz in diese Richtung verfolgt hinsichtlich der Sicherheitsbeurteilung von kritischen Infrastrukturen das EU-geförderte Forschungsprojekt *CyberWiz* [3], das ein Teil des EU Forschungs- und Innovationsprogramms *Horizon 2020* ist. Zunächst wird anhand einer Modellspezifikationsmöglichkeit von Cybersystemen eine gegebene kritische Infrastruktur in einem Modell abgebildet. Die Widerstandsfähigkeit dieses Modells gegenüber Angriffen (Resilienz) wird sodann anhand der Eichskala *Zeitdauer bis zur Kompromittierung* (Time to Compromise – TTC) als statistische Größe unter Anwendung einer Monte Carlo – Methode durch zahlreiche Angriffssimulationsläufe ermittelt. Anhand einer aufgeschlüsselten Ergebnisdarstellung lässt sich nun diese Struktur gezielt hinsichtlich der Cybersicherheit verbessern. Diese veränderte Struktur wird nun wiederum erneut hinsichtlich der Resilienz vermessen und wieder verfeinert modifiziert und so weiter bis sich eine ausreichende Zeitdauer bis zur Kompromittierung erzielen lässt. Damit haben wir die Chance die Cybersicherheit einer kritischen Infrastruktur systematisch anhand von Simulationen lernend vervollkommnen zu können und sodann bei befriedigender Erreichung des Sicherheitsniveaus kostensparend und bereits ausgetestet wirksam in die Realität erst umzusetzen.

Heutzutage sind wir in der Lage rein auf Softwarebasis Netzwerke und deren Strukturen zu definieren (SDN Technology) oder zu virtualisieren (Network Virtualization), schon lange können wir Rechner virtualisieren (VM Technology). Moderne KI Technologie beginnend mit *Deep Learning* ermöglicht uns die Konstruktion von aus Lernvorgängen selbst-adaptierenden Systemen. Eine Orchestrierung aller dieser Mittel könnte bewerkstelligen mit vielen Austestungen evolutionär lernend von Testlauf zu Testlauf die Resilienz systematisch zu steigern (das ist Anti-Fragilität pur!). Wir sind also gar nicht mehr so weit davon entfernt eine neue Ära von sicheren Informationstechnologie-Systemen einläuten zu können.

Nun ist Anti-Fragilität alles?

Durchaus nicht, neben dem Eigenschaftsprinzip Anti-Fragilität sicherer Informationstechnologie-Systeme gilt es verstärkt auf die Konstruktionsprinzipien von Informationstechnologie-Systemen zu achten. Jetzt schlägt die Stunde von *Secure by Design* (Stichwort: immanente Sicherheit).

Oberste Leitlinie muss dabei sein, dass Sicherheit nicht eine nachträglich eingebaute "Komponente" ist, sondern eine von Anfang an durch Sicherheitsziele und/ oder –bedürfnisse bestimmte, wohlanerkannte Ausrichtung der Entwicklungsanforderungen und des Herstellungsprozesses ist. Bemerkenswert finde ich in diesem Zusammenhang, dass schon bereits 1975 von Jerome H. Saltzer & Michael D. Schröder in ihrer Publikation 'The Protection of Information in Computer Systems' [4] acht wichtige Konstruktionsprinzipien zur Herstellung sicherer Informationstechnologie-Systeme identifiziert wurden:

- Einfachheit der Schutzmechanismen (Economy of Mechanism)
- Ausfallsicherheit erzielende Voreinstellungen (Fail-safe Defaults)
- Vollständige Authentisierung (Complete Mediation)
- Offener, nicht geheim gehaltener Entwurf (Open Design)
- Anwendung eines 4-Augen-Prinzips (Separation of Privilege)
- Auslegung der Berechtigungen am Minimum (Least Privilege)
- Geringstmöglicher Einsatz von einander abhängiger Schutzmechanismen (Least Common Mechanism)
- Orientierung an der psychologischen Akzeptabilität (Psychological Acceptability).

Nun, das war immerhin der Erkenntnisstand aus dem Jahre 1975. Zwischenzeitlich können u.a. weitere, neuere Konstruktionsprinzipien aufgeführt werden:

- Einsatz einer möglichst automatisierten (zeitnahe Alarmierung!) Detektion von Anomalien infolge einer Eindringung (Intrusion Detection System/ IDS)

- Einsatz einer möglichst automatisierten (rasche Reaktionsfähigkeit!) Abwehr entdeckter Angriffe (Intrusion Prevention System/ IPS)

- Prinzip einer mehrstufigen Verteidigung unter Anwendung einer kommunikativen Staffelung in der Tiefe (ermöglicht eine Kommunikation zwischen den einzelnen Verteidigungsebenen über seltsames Verhalten, welche einem unter Anwendung von AI bereitgestelltem Entscheidungs- und Expertensystem dazu dient, entscheiden zu können, ob Schädlichkeit vorliegt und für diesen Fall eine schnelle, die verschiedenen Verteidigungsebenen einbeziehende holistischere Abwehrreaktion generiert, siehe hierzu z.B. einen interessanten Ansatz in diese Richtung von Sophos mit ihrer Orchestration *infinity loop)*

- Identitätsbasierte & gebrauchsorientierte Informationstechnologie-Systeme
  (getreu dem Grundsatz: eine zweifelsfreie Identifikation ist oft die Wurzel aller Sicherheit!)

    - Einsatz einer Mehr-Faktoren-Authentifizierung
      (verschafft eine hohe Barriere gegen Identitätsdiebstahl oder –missbrauch!)

    - Prinzip der situativ geringstmöglichen Berechtigungsausstattung
      (reduziert erheblich die Schadensfähigkeit!)

    - Einsatz eines rollenbasierten Berechtigungskonzepts
      (reduziert die Komplexität bereits im Design!)

- Einsatz von sicheren Entwurfsmustern (Secure Design Patterns)
  (nutzt die Wiederverwendung von sicheren, erprobten Entwurfsmustern!)

- oder gar die Umsetzung eines Sicherheits-attributierten Kommunikationsbeziehungs-konzepts, welches auch bekannter ist unter dem Namen *Jericho-Konzept* [5]
  (Getreu der Weisheit: systemisch gesehen sind für das Verhalten eines Systems die Verknüpfungen unter den System-Objekten viel bedeutungsvoller als die System-Objekte eines Systems selbst!).

Zur Verbreitung dieser Konstruktionsprinzipien in die Fläche gilt es gerade die Hersteller und die Betreiber von Informationstechnologie-Systemen bis hin zu gesetzlich definierten Rahmen-bedingungen in die Pflicht zu nehmen (siehe hierzu auch die aktuellen Ansätze durch das IT-Sicherheitsgesetz und durch die EU-Datenschutzgrundverordnung).

Ein jüngeres Technologiebeispiel für ein *Insecure by Design* sind Smartphones. Erst nach und nach beginnen die Hersteller, diese Werkzeuge massenhafter Sicherheitsdestruktion von der Wurzel her sicherer zu machen (siehe Beginn dieses Ansatzes im Jahre 2013 z.B. durch das Smartphone-Betriebssystem von Blackberry *BlackBerry 10*). Doch schon noch neuere Technologien stehen ante portas als Internet der Dinge (IoT) auf unzureichender Sicherheitsbasis gebaut und betrieben, sich massenhaft ausbreitend in kritischen Infrastrukturen durch eingesetzte Smart Meters (intelligente Stromzähler) oder in Smart Homes verbaut (intelligente Heimsteuerung) oder in nicht allzu ferner Zukunft als selbstfahrende Kraftfahrzeuge, die mit vielfältigen, in großer Anzahl eingesetzten Sensoren in Verbindung mit software-basierten zahlreichen Steuer- und Entscheidungssystemen ausgestattet, im IoT hochvernetzt auf unseren Verkehrssystemen agieren werden. Einen hochinteressanten systemischen Ansatz zur IoT-Absicherung verfolgt hier z.B. VMware mit *micro-segmentation*, indem die mittels Virtualisierung geschaffene zusätzliche Abstraktionsschicht als zentrale Drehscheibe und Monitor für die IoT Security fungiert.

Um mich bei meinen Ausführungen nicht falsch zu verstehen, ich möchte das gängige IT-Sicherheitsmanagement basierend auf dem klassischen IT-Risikomanagement nicht für Reif zur Ausmusterung erklären. Es hat gerade in Hinblick darauf begrenzte Möglichkeiten für Schutzmaßnahmen sinnvoll priorisiert ausrichten und umsetzen zu können seine immensen Vorteile. Aber diese Vorgehensweise hat, wie aus meinen obigen Ausführungen deutlich geworden sein dürfte, systemisch und herstellungs- und Betreiber-bedingt hinsichtlich eines nachhaltigen Erfolgs seine Begrenzungen und bedarf dringend einer Ergänzung durch Ausrichtung nach evolutionären Bewährungs- und reiferen Konstruktionsprinzipien – eben eine nachhaltige komplementäre Resilienz-Strategie.

Wie so oft im Leben der Mix macht's.

Literatur

1. Taleb Nassim Nicolas (2007) *The Black Swan: The Impact of the Highly Improbable*, Random House and Penguin, New York
2. Taleb Nassim Nicolas (2012) *Anti-fragile. Things That Gain from Disorder*, Random House, New York
3. EU-*Horizon 2020*-Projekt *CyberWiz* https://cordis.europa.eu/news/rcn/131134_en.html
4. Saltzer JH, Schroeder MD (1975) siehe http://www.cs.virginia.edu/~evans/cs551/saltzer/
5. TheOpenGroup *Jericho Forum* unter https://www2.opengroup.org/ogsys/catalog/W127 oder siehe dazu eine Konzeptanwendung entwickelt von Google: https://beyondcorp.com/

Zum Autor

Dipl.-Ing. Frank W. Holliday, zertifiziert als TeleTrusT Information Security Professional (T.I.S.P.), CISSP und ISO/IEC 27001 Lead Auditor, ist seit über 15 Jahren im Bereich Informationssicherheit tätig und blickt auf eine über 35 Jahre umfassende Erfahrung in vielfältigen Verwendungen im Bereich IT und Informationssicherheit zurück. Er beschäftigt sich insbesondere mit der Aufsetzung nachhaltig sicherer Informationstechnologie-Systeme. Er ist Mitglied der *Gesellschaft für Informatik e.V.* (GI) und arbeitet in der Fachgruppe *Management von Informationssicherheit (SECMGT)* des GI-Fachbereichs *Sicherheit – Schutz und Zuverlässigkeit*, sowie bei der Arbeitsgruppe *ISM* des *TeleTrusT e.V.* mit.

Kontaktadresse

Frank W. Holliday
Wilhelmstr. 1, D-64853 Otzberg
E-Mail: f.w.holliday@holliday-consulting.de

Copyright-Hinweis

Dieser Artikel ist eine aktualisierte Ausgabe eines unter gleichem Titel erschienen Artikels in der Monatsausgabe Februar 2014 (Band 37 – Heft 1) der GI-Fachzeitschrift *Informatik Spektrum* (siehe auch unter link.springer.com).