Vernetzung und Komplexität

Ein Plädoyer für einen kritischeren Umgang mit dem Thema Vernetzung

Fast täglich berichten die Medien über neue IT-Sicherheitsschwachstellen oder von konkreten Cyber-Angriffen. Die Bandbreite geht dabei von „Sicherheitsexperten haben gleich mehrere Lücken im Mobilfunknetz entdeckt“ über „Hacker stahlen Banken eine Milliarde Dollar“ bis hin zu „Gezielter Angriff auf ein Stahlwerk in Deutschland“ oder „1,6 Milliarden Euro Schaden durch Industriespionage in Österreich“. Ganz abgesehen von den unzähligen Vorfällen im privaten aber auch unternehmerischen Umfeld, die nicht breit publik werden. Gleichzeitig sind in den vergangenen Jahren die Anstrengungen zur Erhöhung der IT-Sicherheit massiv angestiegen, was sich nicht zuletzt auch in einer nationalen Cyber-Sicherheitsstrategie niedergeschlagen hat. Doch warum ist keine Verbesserung zu bemerken bzw. wann wird diese endlich eintreten?

Albert Einstein wird gerne mit

„Probleme kann man niemals mit derselben Denkweise lösen, durch die sie entstanden sind.“

zitiert. Hierin liegt möglicherweise auch die wesentliche Erkenntnis, warum trotz steigender Anstrengungen keine Verbesserung zu beobachten ist. Natürlich gab es in den letzten Jahren wesentliche Fortschritte in der IT-Sicherheit. Jedoch handelt es sich um ein ständiges Hase-Igel-Rennen, da es vorwiegend um Symptombehandlungen geht. Die tiefergründigen Ursachen sind, sofern sie betrachtet werden, nur schwer zu beseitigen, da viele Basistechnologien nie für den heutigen Einsatzzweck konzipiert wurden. Eine nachträgliche Änderung ist jedoch nur mit erheblichem Aufwand möglich, zu denen unter den heutigen wirtschaftlichen Rahmenbedingungen kaum jemand bereit ist. Zum anderen hängen viel zu viele Dinge voneinander ab, die eine Änderung nicht so einfach machen. Müssen wir daher mit diesen Unzulänglichkeiten leben, oder macht es doch Sinn, über mögliche Alternativen nachzudenken?

Sowohl-als-auch-Denken

Um diese Frage beantworten zu können, muss unser bisheriger linearer Entweder-oder-Denkrahmen verlassen werden. Dieser hat sich in der Vergangenheit sehr bewährt und zu unserem gesellschaftlichen Erfolg beigetragen. Jedoch haben sich in den vergangenen Jahren zahlreiche Rahmenbedingungen gravierend verändert. Dadurch stoßen unsere bisherigen Lösungsansätze zunehmend an Grenzen. Lineares Denken basiert auf einfache Ursache-Wirkungs-Beziehungen und vermeidet die Auseinandersetzung mit komplexen Vernetzungen und Wechselwirkungen. Komplexe Herausforderungen werden vereinfacht und in Einzelthemen zerlegt, um sie mit den bisherigen Verfahren analysieren und bearbeiten zu können. Zahlreiche aus dem Ruder gelaufene Großprojekte zeugen davon.

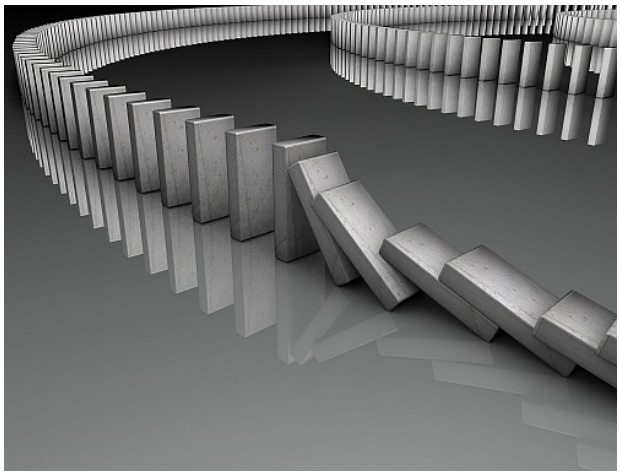
Um jedoch mit den neuen Herausforderungen umgehen zu lernen, muss sich auch unser Denken und Handeln an die neuen, von Menschen geschaffenen, Rahmenbedingungen anpassen. Durch die einfache und kostengünstige Verfügbarkeit von Informations- und Kommunikationstechnik hat die technische Vernetzung mas-

siv zugenommen und ganz unbestritten auch viel Positives geschaffen. Vieles was noch vor wenigen Jahren unvorstellbar war, ist heute selbstverständlich. Viele Erfolge in der Automatisierung und Effizienzsteigerung und damit Produktivitätssteigerung wären ohne diese Errungenschaften nicht möglich gewesen. Jedoch gibt es auch Schattenseiten dieser Entwicklungen, die uns meist nicht so Bewusst sind, da sie häufig erst zeitverzögert auftreten.

Daher ist es notwendig, nicht nur die Vorteile, sondern auch die potentiellen Nachteile von Entwicklungen zu betrachten. Zum anderen wird es auch weiterhin Bereiche geben, wo unser bisheriges lineares Denken ausreichen und erfolgreich sein wird. Jedoch benötigen wir zusätzlich ein vernetztes, systemisches Denken, um auch mit den potenziell negativen Auswirkungen der Vernetzung besser umzugehen lernen.

Vernetzung und Komplexität

Vernetzung führt neben den zahlreichen Vorteilen auch zu Entwicklungen, die uns bisher weniger vertraut sind. So steigt etwa die Komplexität und Dynamik in einem System. Komplexe Systeme weisen eine Reihe von Eigenschaften auf, die wir von unseren bisherigen technischen Lösungen kaum kennen. Es kommt zu nicht-linearen Wirkungen. Eingriffe wirken sich möglicherweise über längere Zeit nicht oder wie intendiert aus. Und scheinbar aus dem Nichts reagiert das System plötzlich völlig unvorhergesehen oder weit heftiger als erwartet. Gerade am Beispiel Finanzsystem ist das immer wieder zu beobachten. Lange Ursache-Wirkungsketten bzw. indirekte und irreversible Wirkungen reduzieren die Berechen- und Steuerbarkeit. Kleine Ursachen können große Wirkungen verursachen, wie folgendes Beispiel zeigt. Der Ausfall eines Steuerrechners in einer Nebenanlage eines großen Produktionsbetriebes führte zu einem Dominoeffekt, der in einem mehrtägigen Betriebsstillstand endete. Aus dem ursprünglichen Schaden in der Höhe von 2.000 Euro entstand ein Folgeschaden in der Höhe von 50 Millionen Euro. Zeitverzögerte Wirkungen können wir auch in der IT-Sicherheit mitverfolgen, wo Schwachstellen oft über Jahre vorhanden sind. Eine wesentliche Rolle spielt dabei, dass durch eine oft nicht zu Ende gedachten Vernetzung die Reichweitenbegrenzungen für Störungen minimiert oder aufgehoben werden. Durch vordergründige Effizienzsteigerungsmaßnahmen entstehen schwer beherrschbare systemische Risiken.



Systemische Risiken

Systemische Risiken sind durch einen hohen Vernetzungsgrad und nicht intendierte Wechselwirkungen mit weitreichenden Dominoeffekten und Nichtlinearität gekennzeichnet. Darüber hinaus werden diese systematisch unterschätzt und in vielen Risikomanagementansätzen nicht ausreichend berücksichtigt, da besonders externe Faktoren zum Tragen kommen. Aufgrund der Seltenheit des bisherigen Eintritts werden sie häufig vernachlässigt und damit völlig unterschätzt. Hier besteht ein Sicherheits- bzw. Verletzlichkeitsparadox. Je sicherer etwas scheint, desto verwundbarer ist es gegenüber großen Störungen, da mit der Zeit auch die erforderlichen Handlungskompetenzen zur Bewältigung von Störungen abnehmen.

Betriebswirtschaftliche Optimierung und Effizienzsteigerung

Während viele Probleme in der Cyber- und IT-Sicherheit ungelöst sind, bzw. durch ständig neue überholt werden, schreitet die technische Vernetzung scheinbar unaufhaltsam voran. Wesentliche Treiber sind dabei betriebswirtschaftliche Überlegungen und der Druck zur Effizienzsteigerung. Dabei wird leicht übersehen, dass ein Widerspruch zwischen Effizienzsteigerung und Systemsicherheit besteht. Betriebswirtschaftliche Optimierungen und Effizienzsteigerungen machen durchaus Sinn, solange sie nicht zum Selbstzweck oder zur reinen Renditenbeschaffung werden. In vielen Bereichen sind wir aber bereits dort angelangt. Immer häufiger werden für die Systemsicherheit wichtige Redundanzen und Reserven eingespart, da sie betriebswirtschaftlich „totes Kapital“ darstellen. Auch beim Fachpersonal wird der Sparstift angesetzt. Immer weniger haben immer mehr zu tun. Die Fehleranfälligkeit und damit die Verwundbarkeit steigen. Wenn sich die Maßnahmen negativ auswirken, ist es meist bereits zu spät bzw. sind schon irreversible oder kostenintensive Folgen eingetreten.

Kritische Infrastruktur und strategische Schocks

Diese Entwicklungen können fast überall beobachtet werden, so auch im Bereich unserer Kritischen Infrastrukturen. Gleichzeitig führt die zunehmende Vernetzung, etwa Stichworte wie „Smart-Metering“, „Smart-Grid“, „Industrie 4.0“ oder „Internet of Things“ dazu, dass immer mehr bisher getrennte Domänen miteinander vernetzt und damit wechselseitig abhängig gemacht werden. Ohne Strom- und Telekommunikationsinfrastruktur geht heute so gut wie gar nichts mehr, oft nicht einmal die Wasserversorgung. Eine europäische Großstörung im Stromversorgungssystem („Blackout“) würde innerhalb weniger Tage zu einem völligen gesellschaftlichen Kollaps führen, wie etwa eine Studie des Deutschen Bundestages zum Schluss kommt. Dabei geht es gar nicht um Worst-Case Szenarien. Bereits ein halbtägiger europaweiter Stromausfall hätte das Potenzial, unsere unvorbereitete und hoch vernetzte Gesellschaft ins Chaos stürzen. Ein solches Ereignis wird zum strategischen Schock und würde unser Zusammenleben nachhaltig verändern.

Wir sind verwundbar, ohne das uns das Bewusst wäre, noch dass wir dafür entsprechende Notfall- und Krisenpläne hätten. Störungen werden ausgeschlossen und sind in vielen Bereichen undenkbar, was jeder Erfahrung widerspricht, wie etwa auch gerade der breit angelegte Angriff auf den Banksektor wieder einmal zeigt. Scheinbar ist es gelungen, durch eine breite Kompromittierung über Banken- und Ländergrenzen hinweg einen Schaden von rund einer Milliarde Dollar zu verursachen. Möglicherweise nur die Spitze des Eisberges, wenn man auf die Erkenntnisse der letzten Jahre zurückblickt.

Wir vertrauen unseren Sicherheitslösungen – zu Recht?

Den neuen Herausforderungen durch die zunehmende IT-Vernetzung im Infrastrukturbereich will man mit entsprechenden Sicherheitslösungen begegnen. Die Frage, warum Lösungen, die bisher im IT-Umfeld nur bedingt erfolgreich waren, im Bereich der Kritischen Infrastruktur mit „more or less of the same“ besser funktionieren sollen, ist bisher unbeantwortet geblieben.

Hinzu kommt, dass im Bereich der Steuerung und Automatisation von Infrastrukturen ganz andere Lebenszyklen als in der klassischen IT-Welt zum Einsatz kommen. Es geht nicht nur um wenige Jahre, sondern oft um mehrere Jahrzehnte. Diese Infrastrukturen müssen über viele Monate ununterbrochen funktionieren und verfügbar sein. Ein Neustart nach einem Sicherheitsupdate, wie das etwa in der IT-Welt üblich ist, ist häufig nicht möglich. Hier prallen gänzlich unterschiedliche Welten und Philosophien aufeinander. Denn es geht nicht nur um

die IT-Infrastruktur oder Software, sondern um die dahinterliegenden Systeme, die damit gesteuert werden.

Eine Warnung sollten auch die zahlreichen erfolgreichen Angriffe gegen die Sicherheitsindustrie sein. Menschen und vor allem Kriminelle sind sehr kreativ: Wenn sich abzeichnet, dass sich der Aufwand lohnen könnte, werden entsprechend hohe Ressourcen eingesetzt. Angreifer verfügen über eine sehr professionelle „Unternehmensstruktur“ und Infrastruktur. Dass es nicht immer nur um Geld geht, zeigt auch die steigende Anzahl von Angriffen auf Infrastrukturen. Breit bekannt gewordene Angriffe, wie der gegen das Iranische Atomprogramm oder der Angriff auf einen deutschen Hochofen stellen dabei nur die Spitze des Eisberges dar.

Das Bewusstsein um die Bedrohungen aus dem Cyberbereich ist in den letzten Jahren deutlich gestiegen. Dennoch stellen diese nur einen Teil der tatsächlichen Bedrohungen für unsere Infrastrukturen dar. Störungen können in vernetzten Systemen durch viele Ereignisse ausgelöst werden. Softwarefehler, Naturereignisse, menschliches Versagen, aber auch exotisch anmutende Ereignisse wie Sonnenstürme können zu weitreichenden Folgen führen. Gerade letztgenannte werden von der OSCE zu den größten globalen Risiken gezählt, sind aber gleichzeitig lokal kaum bekannt. Es geht daher längst nicht nur um Angriffe, wie meist vordergründig diskutiert wird.

„Systemische Risiken werden massiv unterschätzt.“

Wir sind als Gesellschaft durch die Abhängigkeiten von der Kritischen Infrastruktur massiv verwundbar. Das war auch bisher so. Neu ist jedoch, dass die Reichweite der Störbarkeit und die Geschwindigkeit der Ausbreitung in vernetzten Systemen exponentiell zugenommen haben, was etwa auch 2007 die geplatzte amerikanische Immobilienblase gezeigt hat. Kaum jemand hatte die darauffolgenden globalen Schockwellen im Finanz- und Wirtschaftssystem am Radar, geschweige für möglich gehalten.

Es wäre daher blauäugig, diese Tatsachen beiseite zu schieben. Denn die meisten Unternehmen und insbesondere unsere Logistikketten hängen ganz wesentlich von der Verfügbarkeit dieser Infrastrukturen ab. Und somit die ganze Gesellschaft.

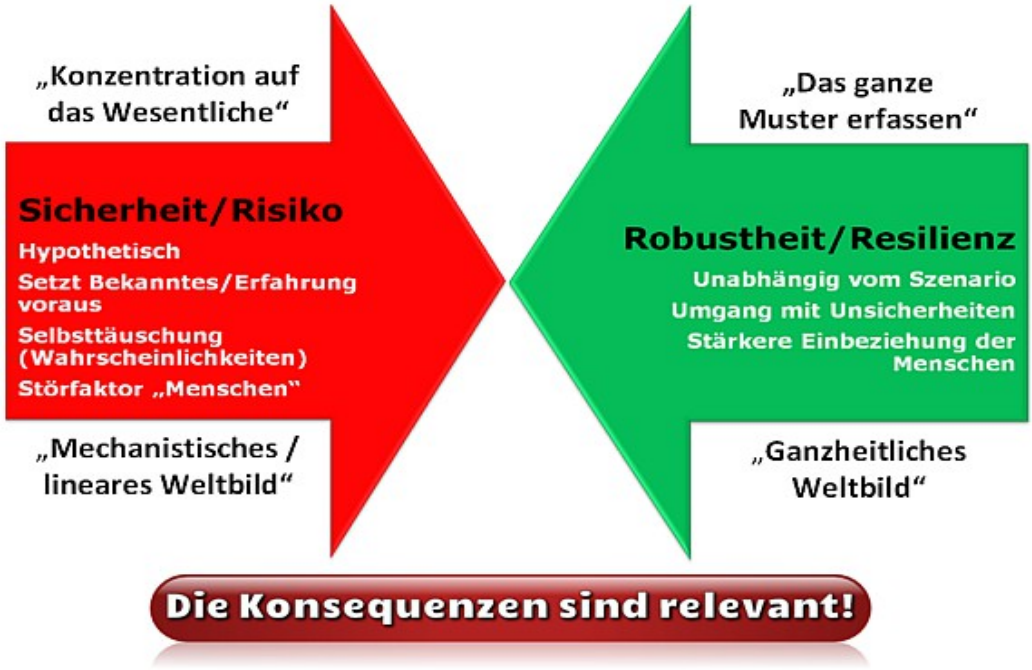
Systemdesign

In der Natur gibt es nur komplexe Systeme und zudem eine sehr lange Entwicklungs- und Erfolgsgeschichte. Grund genug, um von ihr zu lernen. In wenigen Worten lässt sich das auf die Reduktion des Energiebedarfs, die Erhöhung der Fehlerfreundlichkeit und Fehlertoleranz, sowie auf eine dezentrale Steuerung bzw. Regelung zusammenfassen. Damit können Abhängigkeiten deutlich reduziert und die Widerstandsfähigkeit („Resilienz“) des Systems deutlich erhöht werden. Kein Fehler im System darf sich auf das gesamte System negativ auswirken können.

Zellulare Strukturen und Regelkreise, wie sie etwa bereits in der Automatisationstechnik zum Einsatz kommen, sind hier gefragt. Viele derzeitige Konzepte, wie die massive Erhöhung der zentralisierten Vernetzung (Stichwort: Smart), widersprechen diesem Ansatz und führen zu einer unkalkulierbaren Verwundbarkeit.

Sicherheit versus Robustheit

Zum anderen ist es erforderlich, einen neuen Blickwinkel auf das Thema „Sicherheit“ zu werfen. Während unsere bisherigen Sicherheits- und Risikobetrachtungen zur Vorsicht mahnen, fordert der Robustheitsansatz zur Stärke auf. Um die Zuverlässigkeit eines Systems beurteilen zu können, ist eine Risikobeurteilung nur bedingt hilfreich, da diese auf definierte und bekannte Einzelszenarien basiert. Die Feststellung, ob ein System grundsätzlich fragil oder robust ist, lässt auf eine generelle Widerstandsfähigkeit gegenüber Störungen jeglicher Art schließen. Denn während Risiken und Sicherheit hypothetisch sind, ist die Fragilität und Robustheit eines Systems messbar.



Mit der Komplexität steigt auch die Variabilität des Systemverhaltens. Daher ist es notwendig, dass ein System mit möglichst vielen unbekannten Situationen und Störungen umgehen kann. Unsere Kritische Infrastruktur, insbesondere die Stromversorgung, muss daher unter diesen Gesichtspunkten weiterentwickelt werden. Dabei müssen alte, wenn auch bewährte, Denkmuster verlassen werden.

Zusammenfassung

In diesem Beitrag wurde versucht, das Thema IT-Sicherheit aus einem etwas anderen Blickwinkel zu betrachten. Etwa auch mit dem Hinweis, dass Sicherheitstechnik nicht nur zur Lösung beiträgt, sondern auch Teil des Problems sein kann.

Technische Vernetzung schafft nicht nur Vorteile. Die reine Verhinderung von Störungen führt jedoch zu Scheinsicherheit und schiebt den Zeitpunkt von dann kumulierenden Störungen nur hinaus. Daher müssen wir auch mit möglichen (externen) Störungen rechnen und umgehen können. Durch erlebte Erfahrungen aus begrenzten Ereignissen bzw. Übungen kann auch die dafür erforderliche Handlungskompetenz erworben und erhalten werden.

Häufig erlebter Aktionismus ist dabei kontraproduktiv. Statt die Ursache eines Problems zu suchen und dort anzusetzen, wird gerne nur eine Symptombehandlung durchgeführt, da diese rasch angewandt werden kann und ein schnelles („vermarktbares“) Ergebnis liefert. Fundamentale Lösungen hingegen führen kurzfristig häufig zu Nachteilen und bringen erst langfristig einen positiven Nutzen bzw. Mehrwert. Vermeintlich einfachen und raschen Lösungen sollte daher mit einer Portion Skepsis begegnet werden.

Im Umgang mit komplexen Systemen ist vernetztes Denken und Handeln unverzichtbar. Damit werden mögliche externe oder in Wechselbeziehung stehende Faktoren erfassbar und das ganze Muster erkennbar. Zum anderen ist es erforderlich, unser bisheriges Systemdesign generell zu überdenken. Dezentrale Strukturen sind wesentlich robuster gegenüber Störungen und Voraussetzung, um auch mit unvorhersehbaren Ereignissen und Störungen umgehen zu können. „Too-big-to-fail“ ist weder im Finanz- noch im Infrastruktursektor nachhaltig.

Auch wenn wir hier skizzierte Szenarien bisher noch nicht erlebt haben oder uns kaum vorstellen können, stellt sich die Frage, wären wir darauf vorbereitet?

Herbert Saurugg, MSc
kontakt@saurugg.net - www.saurugg.net