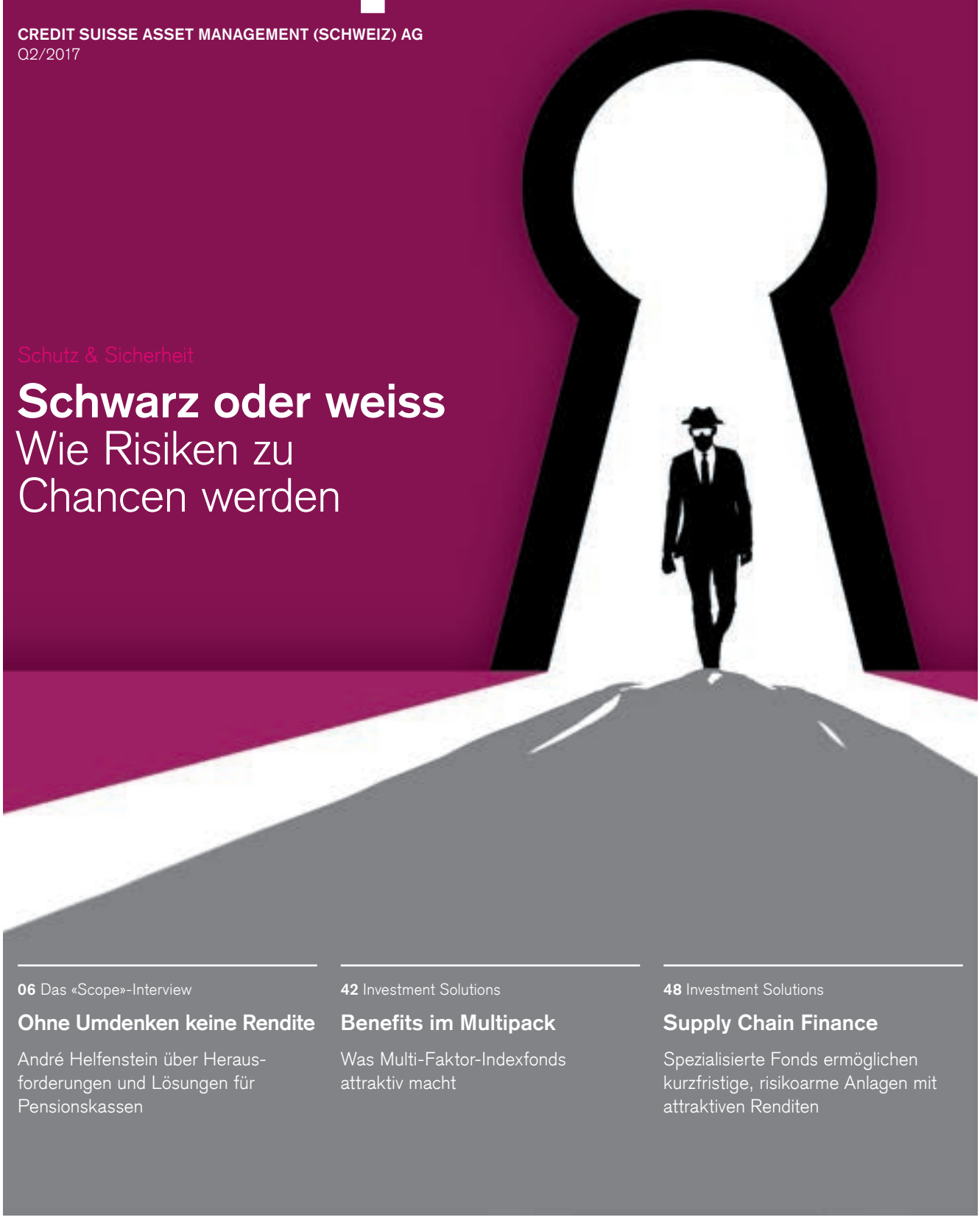
CREDIT SUISSE

Scope

CREDIT SUISSE ASSET MANAGEMENT (SCHWEIZ) AG
Q2/2017



Schutz & Sicherheit

Schwarz oder weiss
Wie Risiken zu Chancen werden

075519D

Cyber Security

Dr. Stefan Frei
Security Principal bei Accenture Cyber Defense,
Dozent für Cyber Security an der ETH Zürich

Das Internet verbindet zunehmend Menschen und Maschinen und hat unser Leben nachhaltig verändert. Die Umwälzungen sind disruptiv, wie damals die Einführung der Eisenbahn oder des Automobils. Dies ist nicht die erste Innovation, welche kritische Fragen zur Sicherheit aufwirft. Neue Möglichkeiten wie auch Bedrohungen entstehen an den Schnittstellen von Technologie, Wirtschaft und Gesellschaft. Welche Lehren der Geschichte können wir auf heute übertragen?

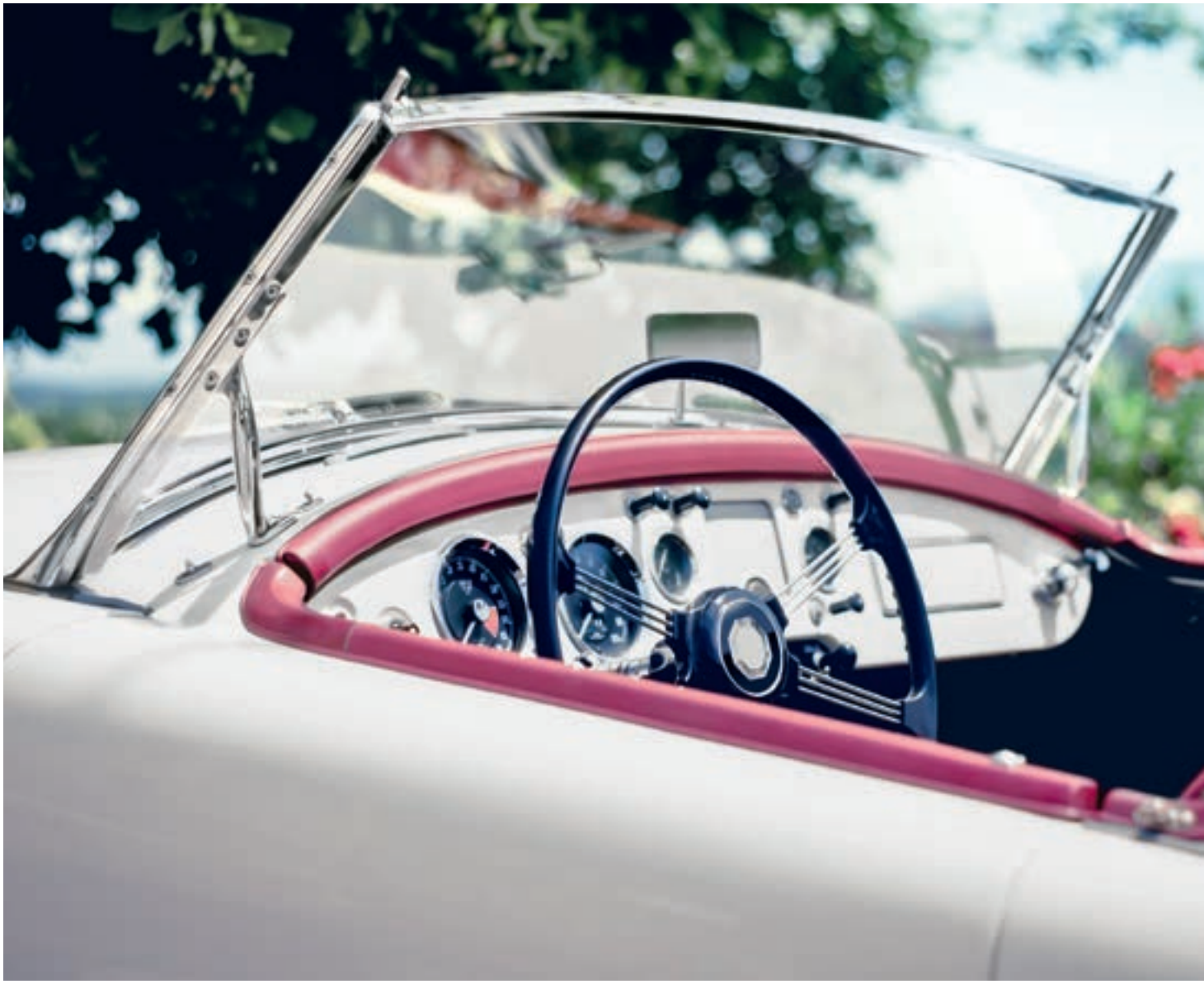
Cyber-Risiken sind abstrakt, haben sich langsam entwickelt und wurden dadurch lange Zeit ignoriert. Digitale Produkte dringen vermehrt in alle Bereiche des Lebens vor und es ist schwierig, Ressourcen zur Abwehr abstrakter Risiken bereitzustellen. Sie werden oft erst nach spektakulären Ereignissen erkannt, mit der Gefahr zu Überreaktionen in der Abwehr.

Software eats the world

Software ist ein bedeutender Treiber dieser Entwicklung. Trotz grosser Investitionen schafft es die Industrie jedoch nicht, sichere Software zu erstellen. Wir müssen uns weiterhin mit Sicherheitsschwachstellen auseinandersetzen, neu auch in Bereichen ausserhalb der traditionellen Softwareindustrie, welche lernen musste, dass das unabhängige Entdecken und Publizieren von Schwachstellen nicht zu verhindern ist. Früher wurden Entdecker von Schwachstellen ignoriert oder mit Rechtsmitteln an der Publikation gehindert. Viele Schwachstellen wurden daher nie oder nur mit grosser Verzögerung repariert, trotz der Risiken. Über die Zeit hat sich der Coordinated-Disclosure-Prozess etabliert: Ethische Entdecker melden die Schwachstelle unter Geheimhaltung zuerst dem Hersteller und geben ihm eine vernünftige Frist zur Entwicklung eines Sicherheitsupdates, bevor die Information publiziert wird. Kooperiert der Hersteller nicht, wird die Schwachstelle sofort publiziert, damit die Betroffenen das Risiko abschätzen können. Die Geschichte lehrt, dass Hersteller nur aufgrund der drohenden Publikation zügig ein Softwareupdate entwickeln. Coordinated Disclosure ist nun zumindest in der Softwareindustrie etabliert.

Durch das Internet of Things (IoT) werden viele Software-ferne Industrien und deren Produkte vernetzt, wobei die Erkenntnisse der Softwareindustrie (sichere Entwicklung, Coordinated Disclosure) oft ignoriert werden. Meldungen über Sicherheitsdefekte in digitalen Stromzählern, Überwachungskameras oder Thermostaten häufen sich.

Warum finden digitale Produkte mit vermeidbaren Sicherheitsdefekten den Weg in den Markt?



Fehlende Produktehaftung
Bei der Einführung einer Innovation (z. B. Automobil, Aviatik) ist die Sicherheit sekundär, Erfahrungen und Sicherheitsnormen fehlen noch. Mit steigender Verbreitung mehren sich die Vorfälle und die Gesellschaft beginnt, die Sicherheit zu hinterfragen. Forderungen nach verbindlichen Sicherheitsnormen werden von den betroffenen Industrien jeweils heftig mit denselben Argumenten bekämpft:

1. Das Produkt ist sicher, Unfälle sind dem Benutzer zuzuschreiben.

2. Sicherheitsnormen sind nicht notwendig, sie würden die Industrie wirtschaftlich ruinieren.

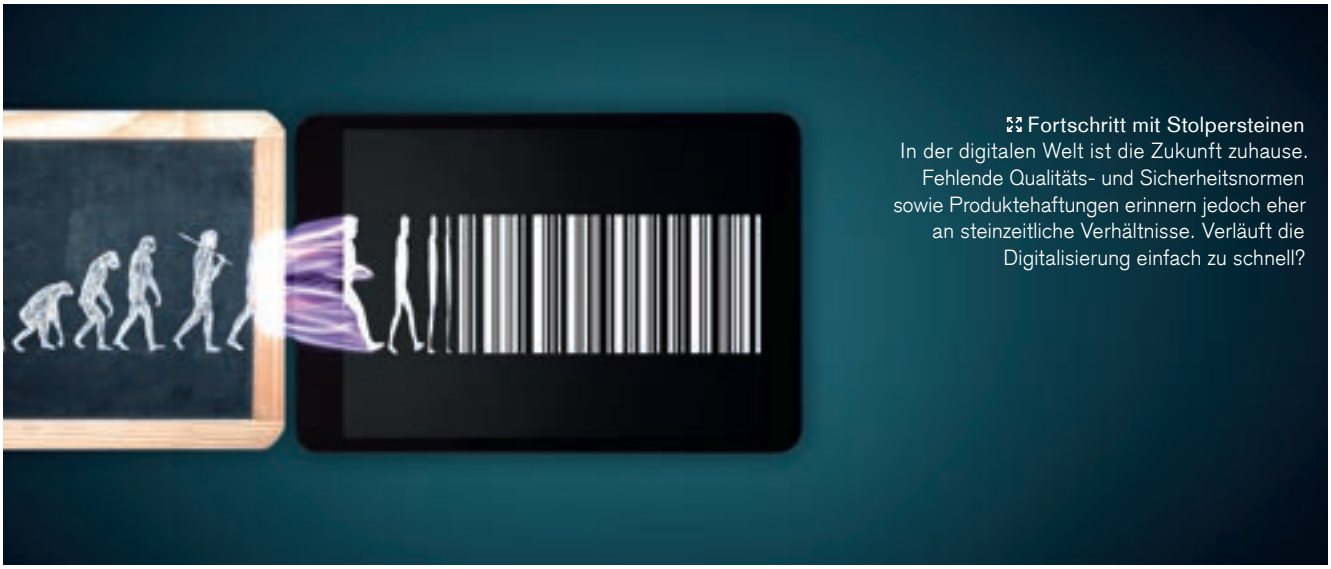
3. Sicherheitsnormen würden die Innovation verunmöglichen.

Ralph Naders Buch «Unsafe at any Speed» von 1965 veranschaulicht diesen Konflikt und führte nach Auseinandersetzungen mit der Automobilindustrie zur Einführung von Sicherheitsgurten und Crashtests sowie zu Produkterückrufen. Die Flugzeugindustrie bekämpfte in der Frühzeit die Tests von Flugmotoren –, über die Hälfte bestanden die ersten Tests anschliessend nicht.

Heute sind fehlende Sicherheitsnormen in diesen Industrien unvorstellbar. Die Automobil- wie auch die Aviatikindustrie bestehen noch und sind massgebliche Innovatoren.

Bei hohem Schadenspotenzial (z. B. Lebensmittel, Pharmazie, Transport, Bauwesen etc.) hat die Gesellschaft jeweils

Nach oben offen
Cyber-Risiken sind abstrakt und schwer erkennbar. Im Automobilbau hingegen sind viele Sicherheitslücken offensichtlich und werden seit 1965 und dem Erscheinen von «Unsafe at any Speed» von den Herstellern wenn irgendwie möglich geschlossen. Dabei leisten Crashtest-Dummys gute Dienste. Das Potenzial für mehr Sicherheit ist in beiden Bereichen offen.



Fortschritt mit Stolpersteinen
In der digitalen Welt ist die Zukunft zuhause. Fehlende Qualitäts- und Sicherheitsnormen sowie Produktehaftungen erinnern jedoch eher an steinzeitliche Verhältnisse. Verläuft die Digitalisierung einfach zu schnell?

Normen zur Qualität und Sicherheit eingeführt, gestützt durch realistische Tests. Das Fehlen solcher Normen für digitale Produkte ist angesichts deren steigender Bedeutung zu hinterfragen.

Es gibt keine Produktehaftung für Software; Sicherheitsupdates sind als Rückrufaktionen fehlerhafter Software zulasten des Kunden zu betrachten.

Verbindliche Normen oder Tests für kritische digitale Produkte sind zu entwickeln, damit auch in Zukunft die Chancen der Digitalisierung ihre Risiken übertreffen.

Traditionelle vs. digitale Produkte
Traditionelle Produkte ändern sich nach der Auslieferung kaum noch, während digitale Produkte fortwährend Sicherheitsupdates benötigen. Viele digitale Produkte haben eine Lebensdauer von Jahrzehnten (z. B. Stromzähler, Kontrollsysteme) und Ersatz, zum Beispiel nach Konkurs des Herstellers, ist kaum möglich oder zu teuer. Ohne Vorkehrungen wie

- der Quellcode wird frei verfügbar (Open Source), sobald der Hersteller ausscheidet
- vor der Anschaffung wird der Quellcode bei einer unabhängigen Stelle deponiert, bei Ausscheidung des Herstellers geht er zum Kunden über

werden kritische Produkte ohne Schutz noch Jahre in Betrieb sein. Viele digitale Produkte sind auch eng mit Backend-Diensten der Hersteller gekoppelt. Wird das Backend nicht mehr weitergeführt, entsteht zum Beispiel für Kontrollsysteme eine kritische Situation. Solche Abhängigkeiten müssen vor dem Einsatz berücksichtigt werden.

Besonderheiten von Cyber-Herausforderungen
Mit der Verbreitung digitaler Produkte treffen wir auf Herausforderungen, die wir erst ansatzweise verstehen. Wir laufen Gefahr, durch den vorschnellen Einsatz Sicherheitsprobleme zu schaffen, welche sich erst langfristig manifestieren und nur mit enormem Aufwand zu korrigieren sind.

Wir sind als Gesellschaft gefordert, bekannte und vermeidbare Fehler zu vermeiden. Verbindliche Normen oder Tests für kritische digitale Produkte sind zu entwickeln, damit auch in Zukunft die Chancen der Digitalisierung ihre Risiken übertreffen.

Dr. Stefan Frei
Seit 20 Jahren beschäftigt sich Stefan Frei mit Cyber Security aus der Sicht des Angreifers wie auch des Verteidigers an der Schnittstelle Gesellschaft, Wirtschaft und Technologie. Er arbeitete im In- und Ausland in den Bereichen Penetration Testing, Defense Effectiveness, Security Architecture und Data Analytics. Bei Accenture Cyber Defense beschäftigt er sich mit Threat Intelligence und fortgeschrittenen End-to-End-Angriffssimulationen zur Unterstützung von Organisationen im Schutz gegen hochentwickelte und gezielte Angriffe.

Accenture Cyber Defense
Als eines der weltweit grössten Beratungshäuser für die digitale Transformation von Unternehmen gilt Accenture als einer der Vorreiter in der proaktiven und ganzheitlichen Implementierung von Cyber Defense in Digitalisierungs- und IT-Projekten. Über 6000 Cyber-Security-Spezialisten sind dazu täglich weltweit im Einsatz. Ein besonderes Augenmerk liegt dabei auf sehr realitätsnahen Ansätzen, welche die reellen und sehr dynamischen Angriffsvektoren aktueller Cyberkriminalität – zum Beispiel auch im Bereich des Internets der Dinge – aufnehmen. Gestützt wird dieses Wissen durch diverse weltweite Forschungszentren und Cyber Fusion Centres in Cyber Security Hotspots wie zum Beispiel Israel.