SICHERHEIT IN TECHNIK UND GESELLSCHAFT

Versorgung mit Lebensmitteln, Wasser, Gas und Strom erfordern eine Vielfalt an verzahnten Technologien. Technik bestimmt Transport, Arbeit, Freizeit und Unterhaltung. Dieser Status Quo ist kein statischer Zustand, sondern verstärkt sich weiter. Dabei nimmt der Anteil digitaler Technik stetig zu. Ein Ausfall von nur wenigen und kleinen Bereichen kann zu Auswirkungen führen, die mehr als nur unangenehm sind (man denke an einen feststeckenden Aufzug) und absichtlich herbeigeführte Störungen können lebensbedrohliche Konsequenzen haben.

BEDROHLICHE KONSEQUENZEN

Computerviren zum Beispiel: Im Frühjahr 2017 sorgte ein Cyber-Angriff durch die Viren „WannaCry“ und „NotPetya“ für erhebliche Gefährdungen in Krankenhäusern. Auch 2018 sind bereits gravierende Vorfälle beim Bund und Probleme beim US-Heimatschutzministerium bekannt geworden. Einer der größten „distributed Denial of Service“ (dDoS)-Angriffe (d.h. viele einzelne Rechner greifen gemeinsam ein Ziel an, um dessen Service lahmzulegen) ist mit „Memcached Reflection Amplification“ im Februar 2018 bekannt geworden. Dabei wurden ausgewählte Ziele mit bis zu 1,7 TBit/s unter Beschuss genommen und damit deren Internetanbindung gesättigt, so dass reguläre Anfragen nicht mehr ihr Ziel erreichen konnten.

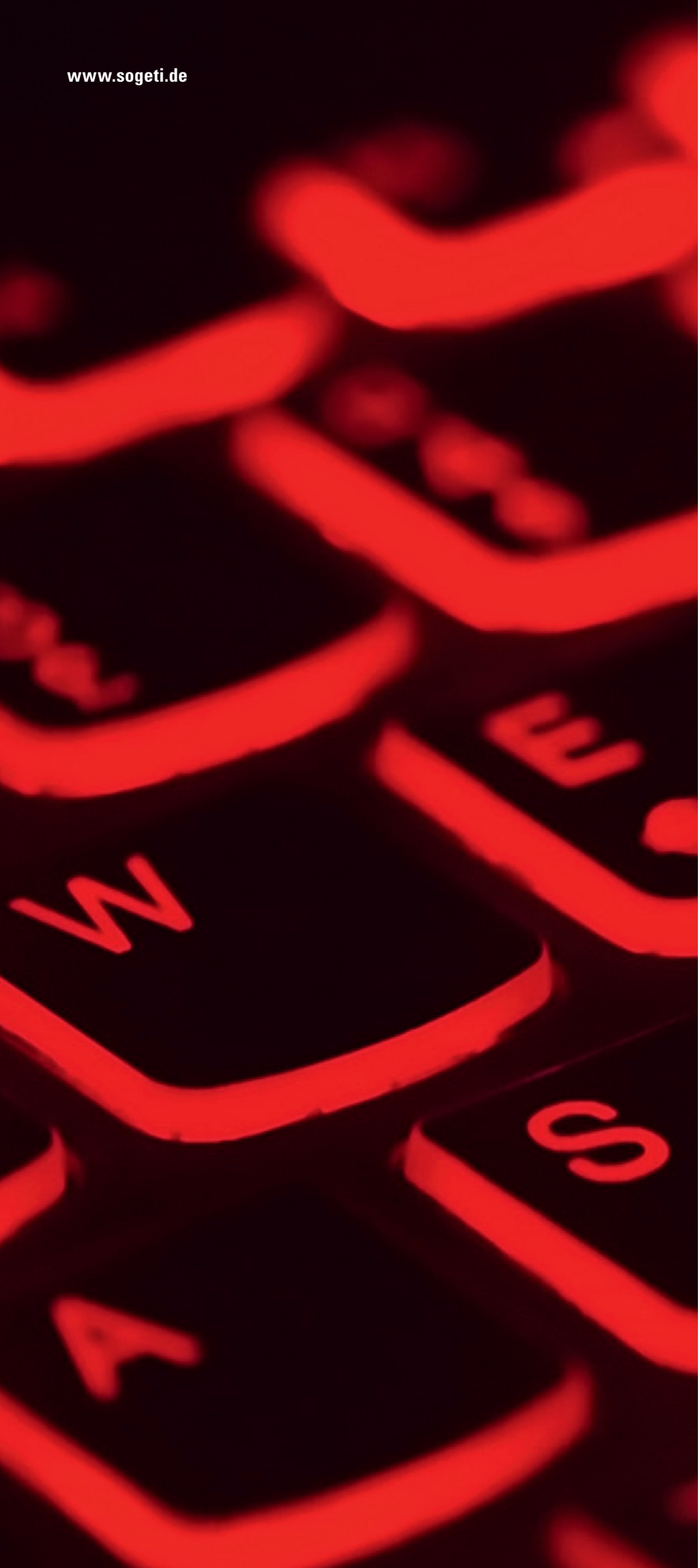
Im März 2018 hat ein Kryptotrojaner das Computernetz der Stadtregierung von Atlanta (USA) lahmgelegt. Welche Auswirkungen ein erfolgreicher Angriff auf die Uhrensynchronisation bei NTP (Network Time Protocol) oder Funkuhren haben kann, ist gar nicht absehbar. Zukünftige „Smart Homes“ mit dem umfangreichen Einsatz des Internet of Things (IoT) bieten ebenfalls lohnende Ziele für Angriffe unterschiedlicher Art. Die Probleme mit dem besonderen elektronischen Anwaltspostfach (beA) sind seit Ende 2017 so gravierend, dass das System abgeschaltet werden musste. Das Thema elektronische Patientenakte steht vor der Tür. Angriffe auf Herzschrittmacher via WLAN wurden schon vor Jahren als „Proof of Concept“ (PoC) demonstriert. Bei der Patientenakte geht es um Verfügbarkeit (auch im Notfall) und um Datenschutz, bei unbefugtem Zugriff auf Herzschrittmacher geht es unmittelbar um Menschenleben.

Je anfälliger die Gesellschaft auf Störungen reagiert, desto intensiver muss Technik abgesichert werden und desto sorgfältiger müssen Menschen mit Technik umgehen. Auch unabsichtliche Fehlbedienungen, möglicherweise provoziert durch unklare Eingabe-Erwartungen, liegen im Blickfeld von Sicherheit. Schließlich ist auch noch die europäische Datenschutz-Grundverordnung (EU-DSGVO) seit Mai 2018 vollständig in

Frank Guthausen hat über drei Jahrzehnte Erfahrungen in den Bereichen Computertechnik, Software-Entwicklung, Administration, Datenschutz und Sicherheit erworben. Derzeit arbeitet er in der Abteilung Cybersecurity bei der Sogeti Deutschland GmbH.

Der Artikel erschien zuerst im SQ-Magazin Nr. 47 | JUNI 2018 **„Security (Testing) in Technik und Gesellschaft“**.

www.sq-magazin.de



Kraft und fordert die Absicherung personenbezogener Daten mindestens nach dem Stand der Technik.

WER IST SCHULD? BLOCKADEN BEI DER SICHERHEIT

Nach dem bisher Gesagten sollte man ein verbreitetes Interesse an Sicherheit in der digitalen Welt vermuten können. Allerdings sind Sicherheitsmaßnahmen nicht direkt sichtbar und Angriffe werden oft nicht direkt wahrgenommen. Dies führt zu einer psychologischen Verdrängung des Problems. Ein vorausplanender Aufwand scheint (gefühlt) unnötig und ist oft aus ökonomischer Sicht schwer zu rechtfertigen. Im Schadensfall kommt es schnell zum „Schwarzer Peter"-Prinzip, in dem das Problem dadurch oberflächlich gelöst wird, indem ein Schuldiger gefunden wird. Auch die gegenteilige Reaktion, in dem gar keiner verantwortlich gemacht wird, weil es „eben passiert ist", ist nicht viel besser.
Das gesellschaftlich verbreitete Dilemma, alles mit einer vergleichenden (eindimensionalen) Metrik bewerten zu wollen, die sich direkt in Geld umrechnen lässt, unterstützt die Sichtweise, es beim Thema Sicherheit nicht so genau zu nehmen. Auf Management- und Führungsebene zählen Umsatz und Gewinn und unnötige Kosten sind zu vermeiden. Bei Fragen zur Sicherheit fehlen klare Ansagen, was nötig und was unnötig ist. Es fehlt eine genaue Definition von Sicherheit.

Administratoren von Systemen haben aus technischer Sicht meist ein ausgeprägtes Verständnis für die Notwendigkeit von Sicherheit. Auf der Ebene des Managements fehlt dieses Verständnis häufig oder ist nur schwach ausgebildet. Und wie sieht es bei der größten Gruppe, den Anwendern, aus? Hier darf man ohne Übertreibung annehmen, dass das Interesse und Verständnis für Hintergrund und

Umsetzung von Maßnahmen aller Art beim größten Teil allenfalls rudimentär oder gar nicht vorhanden ist.

Man denke an unsichere Passwörter für das private E-Mail-Postfach, die dann (zur Sicherheit) noch zusätzlich auf einem kleinen Zettel an den Monitor geklebt werden. Oder das Passwort-Sharing, bei dem sich mehrere Kollegen einen Account teilen und dementsprechend das Passwort kennen – beispielsweise in Krankenhäusern. Das Benutzen unverschlüsselter HTTP-Verbindungen gehört ebenso zum guten Ton wie das Ignorieren von Zertifikatswarnungen bei der Nutzung von HTTPS. Vom regelmäßigen Austausch abgelaufener Zertifikate auf IoT-Geräten fangen wir besser erst gar nicht an.

In vielen Fällen ist der Anwender allein nicht schuld. Oft haben Hersteller allzu viel Sicherheit auch gar nicht vorgesehen. Kommunikation zu verschlüsseln ist grundsätzlich „zu schwierig". Wir haben uns einmal die Produkte eines führenden Software-Herstellers angesehen und müssen vermuten, dass die Lücken in der Sicherheit nicht nur übersehen worden, sondern auch gewollt sind – und auch gar nicht gestopft werden sollen. Zieht man Beobachtungen aus dem privaten Bereich, der freien Wirtschaft und dem öffentlichen Dienst zu Rate, haben die Enthüllungen von Edward Snowden zu den Aktivitäten des US-Geheimdienstes NSA offensichtlich nie stattgefunden. Man sollte vermuten, dass wenigstens die ökonomische Vernunft zu einer Absicherung gegen Wirtschaftsspionage führt, aber selbst auf diesem Feld geht allenfalls von Optimisten noch Hoffnung aus.

VERIFIZIERUNG VON BERECHTIGUNGEN

Bei zugriffsgesicherten Systemen gibt es grundsätzlich drei Methoden, eine Berechtigung zu verifizieren: ich weiß etwas, ich besitze etwas und ich bin etwas. Das Wissen um Passwörter kann belauscht oder abgepresst werden, der Besitzer von Smartcards kann wechseln. So bleibt scheinbar nur ein biometrisches Merkmal. Um eine Person ohne „False Positive" eindeutig zu authentifizieren, muss das System das Gesicht der Person „erkennen". Von „False Positive" spricht man in der IT, wenn ein System einen Fehlalarm auslöst oder fälschlicherweise das System dicht macht.
Leider ist auch diese Methode problematisch. Die grundsätzliche Idee kam nach der Jahrtausendwende immer stärker in Mode und resultierte u.a. in der Aufnahme biometrischer Merkmale in Reisepass und Personalausweis. Wie verschiedene Forschungsergebnisse auch und gerade aus dem Umfeld des Chaos Computer Clubs (CCC) in den letzten Jahren gezeigt haben, sind Verfahren wie Gesichtserkennung, Fingerabdruck-Scan oder Iris-Scan mit haushaltsüblichen Mitteln einfach zu überlisten. Anders als ein Passwort oder eine Smartcard sind biometrische Merkmale aber nicht austauschbar, sondern unveränderlich an die Person gebunden. Eine Kompromittierung ist daher ein sehr schwerwiegendes Vergehen. Unklar ist, ob es sich bei biometrischen Merkmalen um personenbezogene Daten im Sinne der EU-DSGVO handelt, möglicherweise sogar um besonders schützenswerte.

GEFAHR: DER ANWENDER VERLIERT DEN ÜBERBLICK

Bei passwortgeschützten Systemen gibt es oftmals Richtlinien, welche die Sicherheit erhöhen sollen. Dazu gehören regelmäßige Passwortwechsel und die Verwendung von Sonderzeichen sowie der Ausschluss von Wörterbuch-Begriffen. Doch wie soll man sich die steigende Anzahl von Passwörtern merken? Man zähle einmal durch: Pins für Mobiltelefone, Bankkarten, Logins für Privatrechner, private E-Mail, Firmenrechner, Firmentelefon, Social-Media-Accounts. Das überfordert nicht nur durchschnittliche Anwender. Die gängigen Gegenmaßnahmen sind Post-its mit Passwörtern unter der Tastatur oder am Monitor, kleine Gedankenstützen in Schubladen und im Telefonspeicher. Eine weitere beliebte Strategie ist, das gleiche Passwort für alle möglichen Accounts zu verwenden. Das hebelt natürlich den beabsichtigten Schutz aus. Hier begreift die IT nicht, dass Sicherheit an dieser Stelle weder ein technisches noch organisatorisches, sondern ein psychologisches Problem ist. Mehrfaktor-Authentifizierung mit Token und generierten Einmal-Berechtigungen sind da wesentlich wirkungsvoller. Leider verursachen diese aber wiederum Kosten.

KRYPTOGRAFIE: KOMPLIZIERT, ABER EINE LÖSUNG

Ebenfalls Opfer von Überforderung und Bequemlichkeit werden Verfahren zur Verschlüsselung bei Kommunikation und Datenhaltung. Während sich Festplattenverschlüsselung auch außerhalb von Nischenbranchen langsam durchsetzt, ist eine zuverlässige Verschlüsselung von E-Mails nicht selbstverständlich. Mit OpenPGP und S/MIME gibt es zwei große nicht kompatible Verschlüsselungsstandards und die Unterstützung durch Software ist nicht einheitlich. Durch firmeninterne Vorgaben zur Verwendung und Nichtverwendung bestimmter Software ergeben sich weitere praktische Probleme.

Auch bei der Datenübertragung per Webbrowser hat sich HTTPS als verschlüsseltes Protokoll noch nicht vollständig gegen HTTP durchgesetzt. Ein Mitlesen durch Unbefugte kann dabei weder verhindert noch festgestellt werden. Hier ist allerdings durch die Initiative „Let's Encrypt" in den letzten

zwei Jahren ein deutlicher Fortschritt zu erkennen – zumindest, wenn domainvalidierte Zertifikate ausreichen. Extended Validation kostet dagegen zusätzliches Geld. Die Verwaltung von Zertifikaten wird nicht immer sorgfältig vorgenommen. Das Ergebnis sind häufig abgelaufene und ungültige Zertifikate. Revocation, also die Sperrliste für Zertifikate, wird meistens erst gar nicht geprüft. Solche Probleme betreffen neben der Wirtschaft auch den Staat: Selbst grundsätzlich zulässige Abfragen von Sicherheitsbehörden bei einem Berliner Mailprovider liefen im Jahr 2018 noch unverschlüsselt über das öffentliche Netz.

MONOKULTUREN UND HOMOGENE UMGEBUNGEN

Ein weiteres Problemfeld sind proprietäre Monokulturen und homogene Umgebungen. Das Netzwerk der Deutschen Bundesregierung hat eine solche kritische Infrastruktur und wurde deshalb Anfang 2018 auch Ziel eines großen Hackerangriffs. Was zunächst nach administrativer Vereinfachung aussieht, kann bei einem tatsächlichen Sicherheitsproblem statt zu einem Teilausfall gleich zu einem Totalausfall führen. Auch die Abhängigkeit vom Hersteller bei Updates und Sicherheitspatches verhindert eine schnelle, individuelle Reaktion, selbst wenn hochqualifiziertes Personal vor Ort ist. Das Outsourcen von Verantwortung kann zum gefährlichen Bumerang werden. Mit der Cloud werden zusätzlich Daten in den Verantwortungsbereich von Dritten geschoben. Hier hat man es mit einer tickenden Zeitbombe zu tun!

Aktive Angriffe richten sich nicht immer gegen technische Systeme. Auch Menschen sind Ziele. Über Spam, Viren- und Phishing-Mails sollen Mitarbeiter oder Privatpersonen motiviert werden, aus Unkenntnis Handlungen zu ihrem Nachteil auszuführen. Aufklärung und Schulung sind unabdingbar. Niemand ist davor gefeit: Im April 2018 wurde der Autor selbst Ziel einer Social-Engineering-Attacke. Ein angeblicher Mitarbeiter von Microsoft Technical Support berichtete telefonisch von einem identifizierten Problem und kritischen Dateien auf dessen Computer. Anschließend forderte er die Freigabe für den Zugriff auf den Computer. Allerdings ohne Erfolg. Es ist vorstellbar, dass weniger erfahrene Computer-User auf solche hinterhältigen Attacken hereinfallen könnten. Man kann sich denken, was ein solcher „Microsoft-Mitarbeiter" auf einem fremden Rechner anstellen wird.

FAZIT

Das Thema Sicherheit ist kein Puderzucker, den man zusätzlich auf Prozesse und Technologie oben drüber streut. Sicherheit ist auf vielfältige Weise tief verankert und kann nicht überschätzt werden. Ein gesellschaftlich breit aufgestelltes Bewusstsein für die Problematik, ähnlich wie beim Brandschutz, ist längst überfällig. ■