

# Stand der Sicherheit

Von Markus Linnemann, Gelsenkirchen

Sind wir sicher? Beim Autofahren passieren Unglücke, der ICE hat Probleme mit den Achsen und die Zahl der Einbrüche soll im letzten Jahr wieder gestiegen sein. Doch der Bürger fühlt sich sicher, weil er das richtige Auto fährt und seine Haustür gut abschließt und der Bahn vertraut, dass die das Problem mit den Achsen schon in den Griff bekommt. Sicherheit scheint eine subjektive Empfindung zu sein und mit der Bereitschaft zusammenzuhängen ein Risiko einzugehen.

Unternehmen gehen Risiken ein, um handlungsfähig zu sein: Das Werksgelände wird aber gemäß einer Risikoabschätzung geschützt und präpariert – mit Zugangskontrollen, Zäunen und Security-Personal.

In der virtuellen Welt ist der Begriff der Sicherheit weniger greifbar; eine Firewall ist nicht so offensichtlich wie ein Pförtner oder ein Zaun. Es werden zwar Sicherheitsvorkehrungen ergriffen, etwa durch den Einsatz von Firewalls und Anti-Viren-Lösungen, aber reichen diese? Die virtuelle Welt bietet aufgrund ihrer verteilten Struktur nicht nur Vorteile für die Unternehmen, sondern auch für die Angreifer: Der Aktionsradius erweitert sich auf die ganze Welt, während bei einem „physischen“ Angriff die Anwesenheit am Zielobjekt notwendig war. Damit steigt auch die Zahl der potenziellen Angreifer.

## Reaktion meist ungenügend

Wird diesem Risikopotenzial mit geeigneten Mitteln entsprochen? Die Antwort auf diese Frage lautet fast überall: Nein! Dafür gibt es mehrere Gründe: Die digitalen Medien sind den meisten Nutzern noch nicht so vertraut, wie es für die Vielzahl von Anwendungen notwendig wäre. Der

Mensch ist demnach die größte Fehlerquelle, wie es in der realen Welt größtenteils auch der Fall ist. Durch die rasante Entwicklung und die unendlich scheinenden Möglichkeiten gab es bisher nicht genügend Zeit, um Erfahrungswerte aufzubauen – wie beispielsweise bei der Sicherheit von Autos oder dem Verhalten im Straßenverkehr. Es gibt (bislang) keine digitale Sicherheitskultur! Das gilt für alle „digitalen“ Einsatzformen und insbesondere für das Internet.

Ziel muss es also sein, eine Sicherheitskultur für die neuen Medien aufzubauen! Ein glänzendes Beispiel ist eine Umfrage, die das Institut für Internet-Sicherheit if(is) vor Kurzem durchgeführt hat: Auf der Straße wurden Passanten unter einem Vorwand nach ihren Passwörtern gefragt und mehr als 90 % der Befragten gaben ein oder mehrere Passwörter heraus. Auf Nachfrage wurden zusätzlich auch Adressdaten und zugehörige Accounts genannt und es war erschreckend einfach an diese Informationen zu kommen. Hätte man die Menschen nach ihrem Haustürschlüssel gefragt, wäre das Ergebnis ganz sicher anders ausgefallen. Die Sensibilisierung spielt also eine entscheidende Rolle für die Sicherheit im digitalen Umfeld.

Auf technologischer Ebene gibt es heute bereits gute Lösungen, um Sicherheit zu implementieren: Hier bleibt jedoch festzustellen, dass das Bewusstsein, dass digitale Sicherheit Geld kostet, bei den meisten Firmen noch nicht vorhanden ist. Es wird zu wenig investiert, wahrscheinlich nicht zuletzt, weil digitale Sicherheit schwer zu sehen ist und man nicht gerne Geld für etwas ausgibt, das man nicht sehen kann. Meist richtet man erst entscheidende Sicherheitsvorkehrungen ein, wenn zum ersten Mal etwas passiert ist. Diese Einstellung muss sich ändern!

Wichtig ist die Installation von garantierter Vertrauenswürdigkeit. Die kann nur erreicht werden, wenn wir sichere Zustände herstellen und kontrollieren können, ob diese sich verändert haben. Nicht nur Anwender, auch Geräte müssen sich vertrauenswürdig darstellen: Erreichbar ist dieses Level an Vertrauenswürdigkeit über Messwerte. Technologien wie Trusted Computing bieten diese Möglichkeiten frei nach dem Motto: „You can manage it, if you can measure it.“ Hierin liegt ein Schritt von reaktiver Sicherheit zu „proaktiver“ Sicherheit, wie sie mit dem Einbau eines Airbags oder von ESP in der Automobilwelt vergleichbar ist.

## Umfassende Sicherheitskultur

Um in der digitalen Welt sicher zu sein, bedarf es einer Sicherheitskultur, welche die Bewusstseinsbildung der Anwender ebenso umfasst wie die Einsicht, notwendige finanzielle Maßnahmen zu ergreifen. Dazu zählen einerseits Investitionen in digitale Technik und Infrastruktur, andererseits Investitionen in den Einsatz neuer Technologie, die Sicherheit messbar macht und so Vertrauenswürdigkeit herstellt. ■

Markus Linnemann ([markus.linnemann@internet-sicherheit.de](mailto:markus.linnemann@internet-sicherheit.de)) ist Geschäftsführer des if(is) – Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen.

