Der Wettlauf vom Cyber-Igel und Cyber-Hase um die sichere IT.

Kommunen als zweiter Sieger?

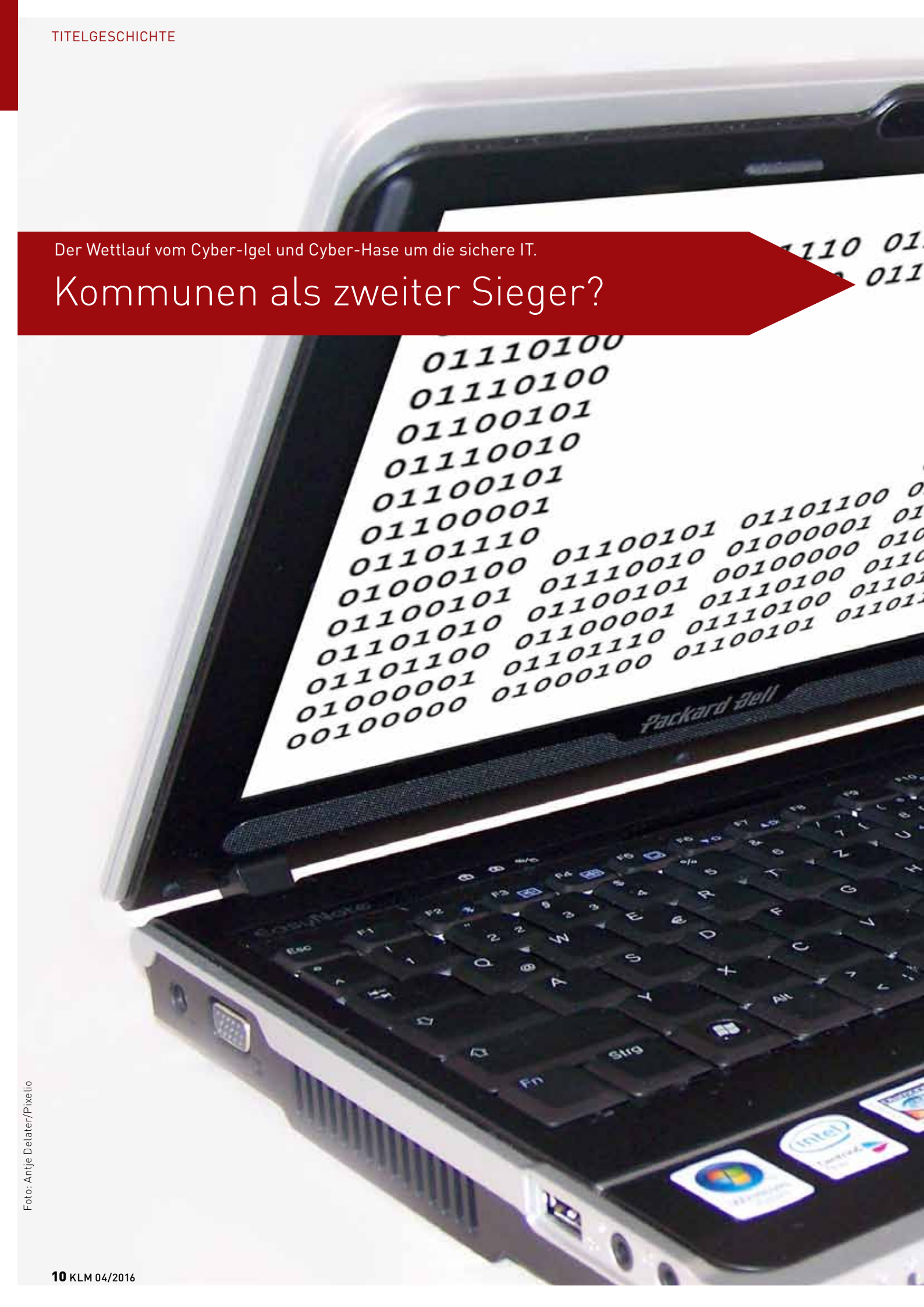

Foto: Antje Delater/Pixelio

Wenn wir in der Vergangenheit an das Thema Hacker gedacht haben, sind uns in der Regel Szenarien eingefallen wie etwa Wirtschaftsspionage – manch einer wundert sich, in China Automobile zu finden, die europäischen optisch sehr ähnlich sind – oder die Versuche des Ausspähens der Passwörter inklusive des Online-Banking-Zugriffs auf dem privaten Rechner.

2013 enthüllte der ehemalige Geheimdienstmitarbeiter Edward Snowden die internationalen Überwachungsaktivitäten der National Security Agency (NSA), die seit spätestens 2007 in großem Umfang die Telekommunikation und dabei insbesondere das Internet verdachtsunabhängig überwacht haben soll.

Und heute im Jahr 2015? Die Digitalisierung unserer Arbeitswelt schreitet rasant voran, jeder ist mit jedem, alles anscheinend mit allem vernetzt. Stichworte dazu sind Social Media Networks, B2B (business to business), B2C (business to consumer), Industrie 4.0, um nur einige sogenannte „Buzzwords" zu nennen. Die Gründe für mehr oder weniger professionelle Angriffe auf Industrie und Wirtschaft liegen auf der Hand. Wo aber liegen die Interessen der Angreifer auf die öffentliche Hand?

Können macht Spaß, Wissen ist Macht.

Die Frage nach den Gründen für Angriffe stellt sich jedoch erst an zweiter Stelle, die jüngste Vergangenheit lehrt uns, dass die ganze Bandbreite an Interessen – vom einfachen Spieltrieb bis zur professionellen, politischen und wirtschaftlichen Interessen – in vollem Umfang auch auf öffentliche Institutionen zutreffen:

- Computerviren im Bundestag – was wollte der Angreifer?
- Zugriff auf die Server der Kfz-Zulassungsstellen in Hessen und Rheinland-Pfalz – was wollten die Angreifer hiermit erreichen?

Die Kernfrage lautet doch: Wie kann man sich vor Angriffen jeglicher Art schützen? Was ist zu tun, um IT sicherer zu machen, als sie heute ist.

Dabei betrachte ich noch gar nicht den Handlungsbedarf im Rechtsraum. - Stichwort dazu das IT-Sicherheitsgesetz (ITSiG) als Vorschlag der Bundesregierung, einen Mindeststandard für die IT-Sicherheit zu vereinbaren und eine Meldepflicht für IT-Störfälle einzuführen.

Gibt es sichere IT?

Ist IT heute trotz der unzähligen Sicherheitskonzepte und installierten Softwareprodukte nicht sicher genug? Ein einfaches Beispiel: Als Mitarbeiter im Back Office einer Bank bearbeitet und prüft Herr Peter jeden Tag zahlreiche Kreditanträge. Eines Morgens hat er eine E-Mail von einer Person in seinem Postfach, die vorgibt, ihn neulich auf einer Veranstaltung in Berlin kennengelernt zu haben. Tatsächlich war er auch dort, nur an den Absender der Mail kann er sich nicht mehr erinnern, da Herr Peter an diesem Tag mit unzähligen Personen gesprochen hat. Trotzdem klickt er auf den beigefügten Link – plötzlich springt ein Pop-up-Fenster im Browser auf, das Herr Peter, ohne es weiter zu beachten, wegklickt. Es war ein Sicherheitshinweis des Browsers. Damit nimmt das Übel seinen Lauf.

Was nun geschieht, kann sehr vielfältig sein: Zugang zum Netzwerk der Bank, damit die Möglichkeit Passwörter oder Daten auszuspähen. Viel wichtiger als die Beschreibung des möglichen Schadenszenarios ist die Analyse, wie der „Einbruch" trotz IT-Sicherheitssysteme hat stattfinden können: die Unachtsamkeit oder Unaufmerksamkeit des Sachbearbeiters in diesem Beispielfall.

Ungewöhnlich? Sicherlich nicht.

Dieses Beispiel soll verdeutlichen, dass IT-Sicherheit bei jedem Nutzer der Informationstechnologie selbst beginnt. Nur so können IT-Sicherheits-

konzepte, Beobachtung und Abwehrmechanismen wirkungsvoll greifen. Ist also das Benutzerverhalten der Schlüssel zu 100 Prozent IT-Sicherheit?

Bestimmt nicht, denn IT ist von Menschen geschaffen, eine Firewall von Menschen entwickelt und programmiert, und Menschen machen Fehler. Die daraus entstehenden Sicherheitslücken in den Programmen auf allen Rechnern dieser Welt ermöglichen es Hackern, in IT-Systeme und Programme einzudringen - trotz achtsamer Anwender und installierter Schutzmechanismen.

Ein Wettlauf mit der Zeit: Cyber-Hase und Cyber-Igel. Entdeckt der Hacker die Sicherheitslücke, bevor sie geschlossen werden kann?

Locksignal Fördermittel

Gilt das auch für den öffentlichen Dienst? Spätestens seit dem Angriff auf den Bundestag ist klar geworden, dass ausschließlich politische Ziele im Fokus der Hacker stehen mit dem Hintergrund, wirtschaftliche Interessen für das eigene Land zu erzielen.

Beispielsweise werden gezielt Behörden ausspioniert, die Fördermittel vergeben. Hier stellt sich die Frage nach dem „Warum?“ Für andere Nationen ist es wichtig, zu erfahren, welche Unternehmen in Deutschland innovativ am Markt agieren und wachsen. Erste Informationen finden sich hierzu sicher leicht im Netz. Danach sind etwa Fördermittelanträge für wachsende Unternehmen, welche in Bundes- und Landesbehörden bearbeitet werden, ein wichtiger Anhaltspunkt für die Angreifer. Diese Information regen die Angreifer an, ihre Hackerattacken auf Ministerien und Behörden gezielt anzusetzen.

Durch das Ausspionieren von Fördermittelprogrammen, Steuervergünstigungen, Wirtschaftsförderung und Fördermittelanträgen entsteht bei ihnen ein Bild, das weitere Rückschlüsse auf interessante Unternehmen entstehen lässt. Meist interessieren sich die Angreifer für die begünstigten Unternehmen, da diese die einträglichsten und schöpferischsten am Markt sind und folglich Ziele weiterer Angriffe werden.

Gegenmaßnahmen

Der IT-Planungsrat hat daher nun festgeschrieben, dass alle Bundesländer bis 2016 CERT (Computer Emergency Response Team) für ihre Behörden aufbauen müssen. Deren wichtigstes Hindernis in der täglichen Arbeit ist, dass -ähnlich wie in der Industrie - auch die Behörden den Angreifern meist zeitlich hinterherlaufen. Außerdem sind die Geldmittel, welche Behörden aufbringen können, im Vergleich zu den Möglichkeiten der Angreifer, unverhältnismäßig klein. Dementsprechend bedarf es einer weiteren schnellen Bereitstellung von personellen, technischen und finanziellen Mitteln im Öffentlichen Dienst, um dieser Unver- ➜

hältnismäßigkeit Herr zu werden. Die Mittelzuführung gestaltet sich in der Praxis durch die langen Haushaltszeiträume und die festen Strukturen teilweise schwierig.

Was also kann man generell tun, um in diesem immerwährenden Wettrüsten mithalten zu können? Auf jeden Fall müssen alle Maßnahmen - seien sie technischer oder organisatorischer Natur - immer auch im Verhältnis zum konkreten Risiko stehen. Doch genau an dieser Stelle tun sich oft die ersten Schwächen auf: Was sind denn die tatsächlichen Risiken, denen die betreffende IT ausgesetzt ist? Welches sind denn die kritischen Daten, auf welchen Systemen befinden sie sich und welche Auswirkungen hätte ein Verlust an Vertraulichkeit, Integrität oder Verfügbarkeit? All dies sind klassische Fragen, die am Anfang eines Prozesses zur Bewertung, Verbesserung und fortlaufenden Pflege der eigenen IT-Sicherheit stehen.

Zusammen mit verschiedenen anderen Themen, Prozessen und Regelungen entsteht auf diese Weise ein Informationssicherheits-Management System (ISMS). Ob dieses nun bis zur Zertifizierung auf Basis BSI Grundschutz oder ISO 27001 fortgeführt wird, muss im jeweiligen Einzelfall betrachtet werden. Zu allererst muss aber erkannt werden, dass IT-Sicherheit keine Ansammlung von Werkzeugen in Verbindung mit oft entweder unzeitgemäßen oder rein situativ-reaktiven Regeln mehr sein darf. Das ISMS soll in erster Linie dazu dienen, als Rahmenwerk für die IT-Sicherheit das zu ermöglichen, was sie heute sein muss: ein beständiger Prozess, der dem Kreislauf „Plan - Do - Check - Act“ folgt.

Auf alle Fälle ist die Voraussetzung für einen echten Mehrwert dabei immer, dass es sich nicht um ein reines Papierwerk handelt, welches den Bezug zur alltäglichen Wirklichkeit in der Behörde verloren hat. Vielmehr muss es einen Rahmen bieten, der es den Beteiligten ermöglicht, die technischen und organisatorischen Änderungen schneller, erfolgreicher und vor allem immer am konkreten Schutzbedarf orientiert einzusetzen. Auf diese Weise entwickelt sich IT-Sicherheit von einer Sammlung aus Werkzeugen und Regelungen zu einem lebendigen Prozess, der den rasanten Entwicklungen auf der Gegenseite etwas entgegenzusetzen hat.

Ob sich an die Umsetzung eine formale Zertifizierung anschließt oder die bestehenden Leitfäden nur als inhaltliche Hilfestellung verwendet werden, steht auf einem ganz anderen Blatt. Die Frage jedoch, ob Informationssicherheit eines stetig fortgeführten, individuellen Management-Prozesses bedarf, wird von jedem Sicherheitsvorfall aufs Neue eindeutig beantwortet.

Und trotzdem werden wir uns auch weiter erfolgreichen Angriffen und Störfällen ausgesetzt sehen, dem Cyber-Hasen und dem Cyber-Igel.

Jörg Prings leitet den Geschäftsbereich Öffentlicher Dienst der PROFI Engineering Systems AG.

Die PROFI Engineering Systems AG

ist ein mittelständisches Systemhaus mit über 350 Mitarbeitern an 15 Standorten in ganz Deutschland. Seit über 30 Jahren unterstützt der IT-Dienstleister branchenübergreifend Kunden mit individuellen IT-Lösungen. Für die Spezialisten der PROFI AG bedeutet Sicherheit in der IT die Implementierung von Verfahren mit den dazu geeigneten Werkzeugen. Dazu gehören ein sicherer Internetzugang mit Web-Inhaltskontrolle, Spam- und Virenschutz sowie die Verschlüsselung von Daten oder sichere VPN-Vernetzung. Darüber hinaus betreuen sie die Sicherheitssysteme von Kunden und beraten über den BSI-Grundschutz und andere Standards.