Informationssicherheit als integraler Bestandteil aller Unternehmensprozesse

Mit dem seit Juli 2015 gültigen IT-Sicherheitsgesetz hat die Bundesregierung die zentrale Rolle Kritischer Infrastrukturen (KRITIS) – wie Strom- und Wasserversorgung, Finanzen, Telekommunikation und Ernährung – für die Bundesrepublik Deutschland formuliert und in einem Kriterienkatalog branchenspezifische Sicherheitsstandards definiert. „et" sprach mit dem IT-Sicherheitsbeauftragten der SIV.AG, Dr. Sebastian Unger, darüber, ob die staatlichen Vorgaben ausreichen, wie Unternehmen sich und ihre Kunden angemessen schützen können und welche weiteren Herausforderungen sich für KRITIS-Unternehmen ergeben.

„et": *Vor dem Hintergrund des Kriterienkatalogs für die Kategorie KRITIS – sind die Unternehmen heute schon gut und ausreichend gegen Betriebsstörungen und Anlagenausfälle geschützt?*

Unger: Die Verpflichtung für Unternehmen des KRITIS-Sektors, sich mit ihrer Informationssicherheit strukturiert auseinanderzusetzen, ist ein sehr wichtiger und guter Schritt in die richtige Richtung. Wir beobachten, dass viele Unternehmen die Leitfäden dankend annehmen und die notwendigen Budgets nun eher freigegeben werden. Häufig jedoch wird die Einführung eines Prozesses zur Aufrechterhaltung der Informationssicherheit auch als lästige, unnötige Pflicht wahrgenommen, die im Wesentlichen Ressourcen kostet, ohne einen Gegenwert zu leisten. Somit können diese Prozesse nicht zum Leben erweckt werden und eines der wichtigsten Ziele – nämlich die Meldepflicht für Sicherheitsvorfälle, um überregionale Muster oder Angriffe erkennen zu können – wird empfindlich geschwächt.

Ich denke, der Grundstein für eine robuste Informationsverarbeitung in den KRITIS-Sektoren ist gelegt. Nun müssen die geschaffenen Strukturen durch kontinuierliche Verbesserungen gefestigt werden, damit die Idee einer deutschlandweiten (und später vielleicht europa- oder weltweiten) Verteidigungslinie gegen Angriffe auf unsere Infrastrukturen Gestalt annimmt.

„et": *Es wird viel über Cyberkriminalität geredet. Was ist besonders gefährdet und warum?*

Unger: Cyberkriminalität betrifft mittlerweile alle Bereiche unseres Lebens. Einbrüche in schlecht gesicherte Online-Shops machen unsere Privatanschrift und unsere Zahlungsinformation zur Ware für Kriminelle. Moderne Spielzeuge übertragen jedes gesprochene Wort in einem Kinderzimmer zur Auswertung an den Hersteller. Banking-Trojaner infizieren unsere Smartphones und PCs, um unsere Konten leerräumen zu können. Das wichtigste Werkzeug für einen Autodiebstahl ist heutzutage eine Richtfunkantenne. Digitale Patientenakten wurden meines Wissens nach noch nicht erfolgreich angegriffen, aber ich denke, auch hier wird es zwangsläufig zu einem Zwischenfall kommen. Und auch unsere kritischsten Infrastrukturen – Strom, Wasser und Telekommunikation – bieten eine wachsende Angriffsfläche.

Die voranschreitende Digitalisierung und Vernetzung gehen einher mit einer steigenden Gefährdung all unserer Lebensbereiche. Wir als Gesellschaft müssen darauf reagieren. Die Politik hat wie oben erwähnt die ersten Schritte bereits unternommen. Als Konsumenten können wir ebenfalls unseren Teil beitragen, indem Produktsicherheit zu einem Kaufkriterium wird.

„et": *Welche Faktoren sind generell bei der IT-Sicherheit zu beachten?*

Unger: Bei IT-Sicherheit wird oft an technische Lösungen wie Antiviren-Software und Firewalls gedacht. Diese Komponenten sind zweifellos notwendig, aber eben nicht hinreichend. Sie können nur effektiv eingesetzt werden, wenn ihnen organisatorische Maßnahmen zur Seite gestellt werden. Wie und unter welchen Bedingungen werden diese Komponenten gewartet? Wird durch Zutrittsregeln und ein Schließsystem der Zugang zu Netzwerkanschlüssen verhindert? Werden Protokolle, die einzelne IT-Komponenten automatisch anlegen, auch nach einem definierten Vorgehen ausgewertet? Ein dritter Aspekt ist weiterhin unerlässlich: IT und IT-Sicherheit betreffen mittlerweile jeden Mitarbeiter eines Unternehmens und entsprechend müssen alle Mitarbeiter regelmäßig geschult werden, um ihnen bestehende Gefahren und ihre Verantwortung dabei zu verdeutlichen.

„et": *Systeme werden zunehmend komplexer, werden sie dadurch auch anfälliger?*

Unger: Das liegt zweifellos in der Natur der Sache. Die Sicherheitsforschung entwickelt immer ausgefeiltere Mechanismen, um Angriffe zu erkennen. Gleichzeitig nutzen Cyber-Kriminelle die Komplexität der angegriffenen Systeme und v. a. der an sie angebundenen Komponenten, um ihre

„Der Grundstein für eine robuste Informationsverarbeitung in den KRITIS-Sektoren ist gelegt. Nun müssen die geschaffenen Strukturen durch kontinuierliche Verbesserungen gefestigt werden, damit die Idee einer deutschlandweiten (und später vielleicht europa- oder weltweiten) Verteidigungslinie gegen Angriffe auf unsere Infrastrukturen Gestalt annimmt."

Dr. Sebastian Unger, IT-Sicherheitsbeauftragter der SIV.AG, Roggentin

Angriffe zu verschleiern. Jüngst wurde bekannt, dass eine verbreitete Malware ihre Befehle von einer Social-Media-Plattform erhielt: Die Kriminellen versteckten die Befehle in scheinbar harmlosen Kommentaren unter Fotos einer bekannten Pop-Sängerin. Für Administratoren des angegriffenen Unternehmens wirkte es, als verbringe ein Mitarbeiter seine Zeit in sozialen Medien. Tatsächlich lud sich die Malware ihre Angriffsbefehle herunter.

Ich glaube, die Komplexität der Einzelsysteme haben wir gut im Griff, solange Hersteller verantwortungsbewusst und offen damit umgehen. Erst die zunehmende Vernetzung einzelner Komponenten zu komplexen, globalen Systemen ermöglichen Nebeneffekte, die vorher nicht bedacht werden konnten.

„et“: *Ist IT-Sicherheit als holistisches Problem zu begreifen?*

Unger: Unbedingt. Nicht umsonst schwenkt die Begrifflichkeit zunehmend von der IT- zur Informationssicherheit. Wie bereits angedeutet, geht es nicht immer nur um IT und Technik, auch wenn das häufig im Zusammenhang mit Informationen der Fall ist.

Informationssicherheit kann nur umfassend funktionieren, wenn sie integraler Bestandteil aller Prozesse eines Unternehmens wird und jeder Mitarbeiter seiner Verantwortung nachkommt. Dadurch wird auch die „Mehrbelastung“ für den einzelnen sehr gering, da jeder seinen Teil beiträgt.

„et“: *Müssten wir nicht korrekt statt von IT-Sicherheit von IT-Schadensbegrenzung reden?*

Unger: Schadensbegrenzung hat immer etwas Reaktives. Das wird einem strukturierten Informationssicherheitsprozess nicht gerecht. Dennoch haben Sie im Kern Recht, es gibt keine absolute Sicherheit. Effektives Informationssicherheits-Management steht und fällt mit einem kontinuierlichen Risiko-Management. Insofern gilt es immer, eine Balance zwischen den Risiken, der Handlungsfähigkeit des Unternehmens und der Wirtschaftlichkeit der erforderlichen Maßnahmen zu finden.

„et“: *Sie arbeiten mit einem Reifegradmodell als Orientierungshilfe für die Branche. Welche Kenntnisse gewinnen Versorger aus einem solchen Modell?*

Unger: Die Entwicklung des Reifegradmodells basiert auf der Erkenntnis, dass sich viele unserer Kunden dem Thema früher genähert hätten, wenn sie einen passenden Einstieg gefunden hätten. Aus eigener Erfahrung wissen wir, wie überwältigend die Herausforderungen zu Beginn sein können. Das Reifegradmodell dient dabei der eigenen Positionsbestimmung. Hat man sich darin einmal wiedergefunden, so gibt das Modell Handlungsempfehlungen. Diese sind auf die Anforderungen der Unternehmen der Energie- und Wasserversorgung abgestimmt und orientieren sich dicht an der ISO 27001, da eine erfolgreiche Zertifizierung häufig ein Etappenziel darstellt.

„et“: *Standardisierung ist ein Schlüsselbegriff in der IT-Sicherheit. Was leistet sie?*

Unger: Grundsätzlich dasselbe wie in allen anderen Bereichen auch. Auf standardisierte Verfahren, Prozesse und Technologien zu setzen, ermöglicht es, auf Erfahrungen zurückgreifen zu können, die man selbst nicht machen musste. Sich an Best Practices aus dem Risiko-Management zu orientieren, erspart einem, selbst ein Verfahren erfinden zu müssen. Bereits lange existierende Frameworks zu nutzen garantiert, keine Aspekte zu vergessen. Die ISO 27001 existiert seit 2005 als unabhängiger Standard, ihre Wurzeln reichen noch weiter zurück und basieren zum Teil auf den noch älteren ITIL-Standards. Seit 2005 wurde sie einmal überarbeitet, um neueste Erkenntnisse zu reflektieren, nachdem sie von vielen Unternehmen implementiert wurde. Für vergleichbare Management-Systeme gilt natürlich dasselbe.

„et“: *WannaCry hat die Anfälligkeit von IT-Systemen vorgeführt. Nun stammte dieser Wurm aus dem Werkzeugkoffer der NSA. Wie bewerten Sie das aus KRITIS-Perspektive?*

Unger: Das betrifft die Unternehmen sehr stark. Immer wieder werden Meldungen publik, laut derer Malware direkt auf die zentralen Systeme zur Überwachung und Steuerung technischer Prozesse – die sog. SCADA-Systeme – kritischer Infrastrukturen zielt. Vor einigen Jahren schreckte Stuxnet die Branche auf. Dieser Wurm verbreitete sich global mit dem einen Ziel, Zentrifugen in iranischen Kernkraftwerken zu beschädigen. Jüngste Erkenntnisse deuten darauf hin, dass der Stromausfall in der Ukraine Ende 2016 ebenfalls auf eine spezialisierte Malware zurückgeht.

„et“: *Aber gerät der Staat dann nicht in einen Zielkonflikt, wenn das Schutzinteresse von IT-Systemen nicht oberste Priorität hat?*

Unger: Wenn vor diesem Hintergrund Geheimdienste Lücken entdecken und verheimlichen, um sie selbst ausnutzen zu können, ist das ein Spiel mit dem Feuer. Nur selten funktioniert die Geheimhaltung von Algorithmen oder Lücken nachhaltig. So kann niemand mehr garantieren, dass eine andere Partei sie nicht auch findet – oder vielleicht bereits längst gefunden hat.

„et“: *Herr Unger, vielen Dank für das Gespräch.*

Die Fragen stellte Thomas Falk/„et“-Redaktion