IT-Sicherheit

Tresor für sensible Daten

[14.10.2021] Betreiber kritischer Infrastrukturen (KRITIS) sind verpflichtet, ihre Systeme gegen Störungen jedweder Art abzusichern. Das zugrundeliegende IT-Sicherheitsgesetz nimmt in seiner neuen Fassung die öffentliche Hand nun noch stärker in die Verantwortung.

Cyber-Angriffe auf kritische Infrastrukturen bedrohen nicht mehr nur private Wirtschaftsunternehmen, sondern immer häufiger auch Einrichtungen von Bund, Ländern und Kommunen. Brandgefährlich werden dieses Hacks, wenn gängige Programme ins Visier genommen werden. So hat Microsoft jüngst eine weitere Attacke auf Regierungsstellen und NGOs in mindestens 24 Ländern gemeldet. Bei den Hackern handelt es sich laut dem Konzern um die Gruppe Nobelium, die auch hinter dem SolarWinds-Angriff steckte. Von diesem waren im vergangenen Jahr Organisationen in der ganzen Welt betroffen: Die Hacker luden sich ein kompromittiertes Software-Update herunter, mit dem sie dann monatelang interne Daten ausspionieren konnten.
Im März dieses Jahres drangen Cyber-Kriminelle über Schwachstellen in der Mail-Software von Microsoft wiederum in fremde Netze ein, unter anderem wurden sechs Bundesbehörden Opfer des Angriffs. Die Microsoft-Lücke hat deutsche Organisationen besonders stark getroffen, weil sie oftmals die E-Mail- und Kollaborationsplattform Exchange im eigenen Haus oder in angemieteten Rechenzentren betreiben. Die dabei verwendeten Exchange-Server-Versionen 2013, 2016 und 2019 wurden zum Teil erst mit Verzögerung durch ein Update gesichert.

Gefahr für die öffentliche Sicherheit

Fallen kritische Infrastrukturen zur Versorgung von Bevölkerung und Wirtschaft mit Energie, Wasser, Lebensmitteln, Medizin oder schnellem Internet Hackern zum Opfer, drohen folgenschwere Engpässe und erhebliche Gefahren für die öffentliche Sicherheit. Alle Organisationen, deren Leistungen für das Allgemeinwohl und den Fortbestand der Wirtschaft und Verwaltung in Deutschland unabdingbar sind, unterliegen deshalb den Vorschriften des IT-Sicherheitsgesetzes. Zu den Auflagen gehört es, die IT- und Ausfallsicherheit am aktuellen Stand der Technik auszurichten. Unter die Regelung fallen neben Bundesbehörden auch Städte und Gemeinden sowie kommunale Unternehmen wie Stadtwerke oder Verkehrsbetriebe.
Aktuell hat die Politik das parlamentarische Gesetzgebungsverfahren für die Version 2.0 des IT-Sicherheitsgesetzes (IT-SiG 2.0) beendet. Zwar müssen zentrale Detailvorgaben noch über Verordnungen geregelt werden, nach Unterzeichnung durch den Bundespräsidenten und der Veröffentlichung im Bundesgesetzblatt Ende Mai 2021 können aber bereits jetzt wichtige Teile kurzfristig in Kraft treten. Gleichzeitig ist das IT-Sicherheitsgesetz ein so genanntes Artikel- oder Mantelgesetz und bildet die Grundlage für Veränderungen in zahlreichen anderen regulatorischen Vorgaben wie der Kritisverordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem Energiewirtschaftsgesetz, dem Telemediengesetz oder dem Telekommunikationsgesetz.

Auch mobile Geräte schützen

Das IT-SiG 2.0 stuft nun auch den Bereich Entsorgung als kritische Infrastruktur ein und erweitert damit den Kreis der betroffenen Institutionen. Hintergrund ist, dass Ausfälle oder Beeinträchtigungen im Bereich

der Abfallwirtschaft nicht nur zur massiven Umweltverschmutzung, sondern auch zu einem Anstieg der Seuchengefahr führen können. Daneben verpflichtet die Neufassung Behörden, Stadtverwaltungen und kommunale Einrichtungen, „Systeme zur Angriffserkennung und Angriffsbewältigung“ zu betreiben. Dazu gehören insbesondere SIEM-Lösungen (Security Information and Event Management) für das schnelle Identifizieren von Cyber-Attacken. Kommt es zu Verstößen, werden künftig analog zur Datenschutz-Grundverordnung (DSGVO) Geldbußen von bis zu zwei Millionen Euro für natürliche und 20 Millionen Euro für juristische Personen fällig. Zudem erhält das BSI als zuständige Kontrollbehörde deutlich mehr Rechte für die Überwachung.

Um sich angemessen zu schützen und die Vorgaben des BSI zu erfüllen, müssen KRITIS-Unternehmen geeignete Sicherheitsmaßnahmen für die größten Schwachstellen ergreifen. Das schließt die mobile Kommunikation ein. Viele Angestellte in öffentlichen Einrichtungen wie Stadtwerken, Verkehrsbetrieben oder Flughäfen sind außerhalb ihrer eigentlichen Dienststelle unterwegs. Smartphones und Tablets machen mobiles Arbeiten möglich, stellen die Verantwortlichen jedoch vor zahlreiche Herausforderungen. Das gilt vor allem dann, wenn dienstliche Geräte auch privat oder private Geräte dienstlich genutzt werden. Richtet beispielsweise ein Mitarbeiter auf seinem eigenen Smartphone ein dienstliches Exchange-Konto ein, vermischen sich private und geschäftliche Daten und Kontakte. Ebenso kritisch ist es zu sehen, wenn sensible Dokumente in einer Dropbox oder anderen unsicheren Apps abgelegt werden. Derartige Vorgehensweisen gefährden die Datensicherheit und stellen einen Verstoß gegen die DSGVO dar. Bei einer BYOD-Regelung (Bring Your Own Device) verliert die IT-Abteilung zudem die Kontrolle: Geht das Smartphone verloren oder scheidet der Mitarbeiter aus, kann sie sensible Daten nicht löschen.

Container als Lösung

Behörden und kommunale Einrichtungen benötigen deshalb ein System, das private und dienstliche Daten sowie Apps strikt voneinander abschottet. Realisieren lässt sich dies mit einer so genannten Container-Lösung. Sollte sich ein Angreifer tatsächlich Zugang zum Smartphone oder Tablet verschafft haben, steht er vor einem verschlossenen Tresor: Die Daten und Dokumente sind nach höchsten Standards verschlüsselt und werden auch verschlüsselt übertragen. Der Zugriff auf den dienstlichen Bereich wird durch eine PIN oder biometrische Verfahren wie Touch- und Face-ID abgesichert. Für höchste Sicherheitsansprüche kann der Zugriff zusätzlich mit einer Smartcard geschützt werden. Das ist auch Voraussetzung bei der BSI-Zulassung für „Verschlusssachen – nur für den Dienstgebrauch“ (VS-NfD). Eine Container-Lösung garantiert außerdem die Einhaltung der DSGVO, da keine private App auf dienstliche Kontaktdaten zugreifen kann. Mitarbeiter können zudem keine Daten per Copy-and-Paste in den jeweils anderen Bereich übertragen.

Gerade kommunale Einrichtungen haben jedoch oftmals nicht die personellen Ressourcen, um die Kommunikation ihrer Mitarbeiter mit komplizierten Systemen wie einem Mobile Device Management (MDM) zu schützen. Vor diesem Problem standen auch die baden-württembergischen Stadtwerke Bad Saulgau, die rund 17.000 Einwohner mit Gas, Wasser, Strom, Fernwärme und Breitband versorgen. Die Stadtwerke strebten die Zertifizierung ihres Informationssicherheits-Management-Systems (ISMS) nach ISO 27001 an, eine zentrale Forderung des IT-Sicherheitskatalogs gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. So suchten die IT-Verantwortlichen nach einer Lösung für die mobile Kommunikation, die vor allem Monteuren einen sicheren Zugang zu E-Mail, Kontakten und Intranet ermöglichen sollte.

Die Stadtwerke entschieden sich für die Container-Lösung SecurePIM vom Anbieter Virtual Solution, welche die Einhaltung höchster Sicherheitsstandards gewährleistet. Das System ist leicht zu implementieren und sehr benutzerfreundlich. Der Arbeits- und Support-Aufwand für die IT-Abteilung konnte so deutlich reduziert werden.

()

Dieser Beitrag ist in der Ausgabe September/Oktober 2021 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, IT-Sicherheit, IT-SIG 2.0, KRITIS, Virtual Solution