IT-Sicherheit “made in Germany”

Die Sichtbarkeit deutscher Spitzentechnologie mit staatlicher Unterstützung erhöhen

(BS/Dr. Holger Mühlbauer) IT-Sicherheit ist eine zentrale Bedingung für das Gelingen der Digitalisierung und für Vertrauen in digitale Infrastrukturen. Die Bundesregierung muss die Schutzpflichten aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme als oberste Priorität einer neuen IT-Sicherheitspolitik anerkennen. Infolgedessen sind Maßnahmen zum Ausbau der IT-Sicherheit zu stärken und Maßnahmen, die die IT-Sicherheit zugleich erheblich schwächen, konsequent abzulehnen.

Die IT- und Produktsicherheit in Deutschland ist als wichtiges Qualitätsmerkmal im internationalen Wettbewerb zu stärken. Dabei sind mit rechtlichen Vorgaben Anreize für Unternehmen zu schaffen, beispielsweise mit Zertifizierungen in gute und sichere IT-Lösungen, insbesondere beim Internet der Dinge, zu investieren. Dazu gehören unter anderem Mindestfristen, in denen Anbieter verpflichtet sind, zeitnah Sicherheitsupdates zur Verfügung zu stellen.

Hinsichtlich der Besonderheiten und Risiken vernetzter IT-Systeme müssen bestehende Haftungsregelungen überprüft werden. Insbesondere vertrauenswürdigere, robuste IT-Systeme, die die Probleme “Softwaresicherheit” und “Malwarebefall” adressieren, sollten gefördert werden. IT-Sicherheitslösungen sollten auf starker Kryptografie basieren und im Kern der IT-Systeme verankert sein. Proaktive IT-Sicherheitslösungen für “Industrie 4.0” sollen direkt umgesetzt werden und Deutschland damit eine weltweite Vorreiterrolle in IT-Sicherheit und Vertrauenswürdigkeit in Bezug auf die Leitindustrien übernehmen. Proaktive Lösungen sind ein innovativer Lösungsansatz, zu dem in Deutschland starke nationale Kompetenz vorhanden ist. Eine der zentralen Herausforderungen von Industrie 4.0 wird die Absicherung der vernetzten Automatisierungssysteme gegen Risiken aus dem unsicheren Internet sein: IT-Security, Datenschutz und Safety müssen auf hohem Qualitätsniveau in deutschen Lösungen für Industrie 4.0 etabliert sein. Eine Kombination aus der Industriemarke “Made in Germany”, deutschem Datenschutz und “IT Security made in Germany” (ITSMIG) kann zum neuen Qualitätszeichen werden und somit den Industriestandort und die Exportnation Deutschland im internationalen Vergleich stärken. TeleTrusT sieht in Industrie 4.0 große Chancen und fordert daher schnelles Handeln:

- Besondere Berücksichtigung von Security by Design, Privacy by Design und Safety by Design bei Planung und Entwicklung von Industrie 4.0,
- Förderung einer politischen Allianz zwischen deutscher IT-Sicherheitswirtschaft und deutschem Maschinenbau im Rahmen der Digitalen Agenda der Bundesregierung,
- Durchführung von Maßnahmen zur “Awareness”-Bildung und Schaffung gesetzlicher Rahmenbedingungen zur Umsetzung von IT-Sicherheit in “Industrie 4.0”,
- stärkere Berücksichtigung von IT-Sicherheit und Safety in der Ausbildung von Ingenieuren auch im Maschinenbau.

Dr. Holger Mühlbauer ist Geschäftsführer beim TeleTrusT – Bundesverband IT-Sicherheit e. V.

Foto: BS/TeleTrusT

Staatliche Anreize sollten die Beschaffung und Abschreibung von Investitionen in Zukunftstechnologien fördern. Verbindliche Sicherheitsmindeststandards für Beschaffungen in der öffentlichen Verwaltung bei Kritischen Infrastrukturen sollten das Thema IT-Sicherheit adressieren.

Die Sichtbarkeit deutscher Spitzentechnologie und deutscher Unternehmen in Bezug auf IT-Sicherheit sollte staatlich unterstützt werden.

Insbesondere IT-Sicherheitsprodukte “made in Germany” müssen sich auch weiterhin durch besondere Vertrauenswürdigkeit auszeichnen, um in Zukunft den Digitalisierungsprozess verlässlich umsetzen zu können. Die TeleTrusT-Initiative “IT Security made in Germany” (ITSMIG) und das darauf basierende Qualitätszeichen spiegeln diesen Vertrauenswürdigkeitsanspruch wider.

TeleTrusT hat seine Mitglieder befragt, welche IT-sicherheitsrelevanten Themen die Bundestagsparteien adressieren sollten. Das Ergebnis kennzeichnet die Problemlagen der IT-Sicherheit in Deutschland:

1. Digitale Souveränität: Die Bundesrepublik Deutschland darf ihre technologische Hoheit über kritische IT-Anwendungen nicht verlieren.
2. Es bedarf eines überparteilichen Konzeptes, wie Deutschland Unternehmen davor schützt, über die IT ausgespäht zu werden und Innovationen zu verlieren.
3. Die Nutzung von IT-Sicherheitstechnologie “made in Germany” muss bei Staat, KRITIS und volkswirtschaftlich wichtigen Produktionsunternehmen Präferenz haben.
4. Der deutsche Mittelstand ist bei der digitalen Transformation zu Industrie 4.0 auf politische Unterstützung angewiesen.
5. Digitalisierung darf nicht automatisch den Verlust der Hoheit über vertrauliche Daten bedeuten.
6. Datenschutz “made in Germany” muss ein Standortfaktor sein.
7. Sichere elektronische Identitäten sind das Fundament der Digitalisierung.
8. Der Einsatz von elektronischen Signaturen muss gefördert werden.
9. Anwender müssen im digitalen Umfeld zum Einsatz von Kryptografie motiviert werden.
10. “Bundestrojaner” sind abzulehnen.
11. Die Bundesregierung muss zu einem aktiven, orchestrierenden Part in der Cyber-Sicherheit werden.
12. Die Konsolidierung der IT des Bundes muss ein wichtiger Schritt in der aktuellen und kommenden Legislaturperiode sein.

Software geprüft und für sicher befunden

Landratsamt Landshut erhöht mit Application Whitelisting IT-Sicherheit

(BS/Ralf Buchholz*) Am 8. Februar 2016 ging plötzlich kaum noch etwas in der Stadtverwaltung von Dettelbach – eine Schadsoftware hatte sich aktiviert, die im Anhang einer E-Mail in das System gelangt war. Die Daten auf den Servern waren verschlüsselt, eine Anzeige auf dem Bildschirm forderte zur Zahlung eines Lösegeldes auf. Das sollte dem Landratsamt Landshut nicht passieren – dafür sorgt das Application Whitelisting von SecuLution.

“Wir haben uns das System während einer Online-Präsentation sehr genau angeschaut und ich muss sagen: Die Lösung hat mir von Anfang an gut gefallen”, lobt *Bernhard Wiedemann*, Leiter Sachgebiet Informations- und Kommunikationstechnik. “Der Ansatz, nur Software, die als sicher eingestuft wurde, ausführen zu können, hat uns überzeugt.” Dann ging es auch ganz schnell: Im April 2016 hatte das Landratsamt die Lösung bestellt, Mitte Mai lief sie bereits.

Zudem hat das Landratsamt weitgehende Anstrengungen zur Steigerung der Sicherheit unternommen. Dazu gehören die Einführung eines Informationssicherheitsmanagement-Systems (ISMS) und SecuLution Application Whitelisting als Endpoint-Schutz. Daneben setzt man in Landshut auf eine neue Spam-Firewall als Mail-Filtersystem und ein Firewall-Cluster. Warum kein teurer Virenscanner? “Der verliert zunehmend an Bedeutung”, ist *Wiedemann* überzeugt, “weil er immer nur auf bekannte Bedrohungen reagieren kann. Nur der umgekehrte Ansatz von SecuLution bietet wirklich einen verlässlichen Schutz.”

Das Prinzip des Application Whitelisting, ist einfach: Die Lösung lässt nur Software ausführen, die eindeutig über einen elektronischen Fingerabdruck auf der Whitelist authentifiziert werden kann, alles Unbekannte wird somit blockiert. “Mit SecuLution kann ich also genau steuern, welche Applikationen ich in meinem Netzwerk zulassen möchte. Um die Ausführung von unerwünschter Software zu verhindern, muss ich nichts mehr tun. Das Problem ist durch das Funktionsprinzip von SecuLution automatisch gelöst.”, so *Wiedemann*. So simpel das Prinzip der Lösung, so einfach sei sie auch zu installieren, meint der Sachgebietsleiter: “Wir bekamen von SecuLution eine komplett fertige virtuelle Maschine geliefert. Die haben wir in unser Virtualisierungssystem implementiert und fertig. Anhand der sehr verständlichen Dokumentation konnten wir alles ganz einfach in Betrieb nehmen.” Danach folgten die Konfiguration und eine Schulung durch den Anbieter.

Schließlich ging es darum, dem System beizubringen, welche Anwendungen in Zukunft ausgeführt werden dürfen. Dazu wurde der SecuLution-Server einen Monat lang in den Lernmodus versetzt. Im Lernmodus werden die Anwendungen übernommen, die die Nutzer im Alltag aufrufen. Nach vier Wochen konnte der Lernmodus beendet werden und SecuLution kannte nun auch alle Anwendungen, die zur täglichen Arbeit benötigt werden. “Der gesamte Prozess war ganz einfach und von der Administration her sehr unkompliziert”, lobt *Wiedemann*.

Doch woher weiß man, dass die Software die durch den Lernmodus auf der Whitelist erfasst ist, auch wirklich vertrauenswürdig und sicher ist? Hier hilft die TrustLevel-Datenbank, die SecuLution seinen Kunden zur Verfügung stellt. “Wir prüfen neue Software einfach gegen die Online-Datenbank von SecuLution und können so Schädlinge identifizieren, die im Lernmodus erfasst wurden”, beschreibt *Wiedemann* das Prozedere. Diese Aufgabe fällt ausschließlich Mitarbeitern seiner Abteilung zu, die mit einem Fokus auf IT-Sicherheit geschult sind. “Nach diesem Audit bilden die nun geprüften Programme die endgültige Whitelist auf dem SecuLution-Server und die Software kann genutzt werden”, so der IT-Manager.

Neben dem Zugang zur TrustLevel-Datenbank hat das Landratsamt Landshut ein ganzes Servicepaket bei SecuLution gebucht. Es enthält den Support und zukünftige Updates der Software. “Wir sind zwar mit Ausnahme der Einführungsphase noch nicht häufig in die Verlegenheit gekommen, auf den Support zurückgreifen zu müssen”, sagt *Wiedemann*, “falls es aber doch nötig war, haben wir immer sehr zeitnah Hilfe bekommen. Insbesondere Konfigurationen des SecuLution-Agents, die in unserer Umgebung erforderlich waren, wurden sehr schnell vom Support erklärt und in Zusammenarbeit mit unserem Team umgesetzt. Unserer Erfahrung nach ist auf den Support von SecuLution zu 100 Prozent Verlass.”

Heute sieht sich das Landratsamt Landshut in Bezug auf die IT-Sicherheit recht gut für die Zukunft aufgestellt. Eine Lücke, die der Sachgebietsleiter Informations- und Kommunikationstechnik noch gerne schließen möchte, ist eine Portkontrolle, um den Zugriff von USB-Massenspeichern zu verhindern. “Da werden wir uns in nächster Zeit sicher einmal das SecuLution- Modul für das Whitelisting und die Verschlüsselung von USB-Geräten anschauen”, sagt *Bernhard Wiedemann*.

**Ralf Buchholz ist freier Journalist.*