GEFAHR AUS DEM NETZ

So schützen Unternehmen Produkte und Dienstleistungen

Im Mai 2017 machte die Software WannaCry Schlagzeilen. Das Schadprogramm hatte weltweit Tausende Computer lahmgelegt. Die Folgen waren fatal: Krankenhäuser konnten auf keine Patientenakten zugreifen, Anzeigetafeln der Deutschen Bahn blieben schwarz, Tankstellen konnten keinen Treibstoff verkaufen, Produktionsbetriebe standen still. Wie viel Gefahr droht von Cyberkriminellen? Wie kann man Produkte und Dienstleistungen schützen? Experten aus der Region geben Auskunft.

Birgit Mann*

Foto: Martina Dach

Frank Kargl, Direktor des Instituts für Verteilte Systeme an der Universität Ulm, beschäftigt sich u. a. mit der Sicherheit in Computernetzwerken.

Im Institut für Verteilte Systeme der Universität Ulm beschäftigt sich Frank Kargl, Direktor des Instituts, unter anderem mit der Sicherheit in Verteilten Systemen und Computernetzwerken. „Wir arbeiten am Entwurf sicherer Systeme, zum Beispiel in eingebetteten Systemen in Fahrzeugen oder Industrieanlagen“, konkretisiert er sein Tätigkeitsfeld. Als eingebettete Systeme bezeichnet er Steuerrechner, die mit der realen Welt interagieren. So erfassen etwa Sensoren Daten, die im Steuerrechner verarbeitet werden. Die Funktionsweise findet sich heute in Rasenmährobotern, Fotokameras oder Autos.

„Unsere Arbeit beginnt mit der Analyse von Schwachstellen, die ein Einfallstor für Angriffe bilden könnten. Dann überlegen wir, wie wir Rechner, CPUs und Netzwerke absichern können. Ein Mittel ist die Sicherstellung einer korrekten Kommunikation zwischen den Steuergeräten, wobei die erfassten Daten auch auf ihre Richtigkeit geprüft werden. Dazu arbeiten wir an Systemen, die zum Beispiel gefälschte Messwerte erkennen können“, erklärt Kargl. „Ergänzt werden diese Systeme durch Mechanismen, die die Kommunikation durch kryptografische Verfahren absichern. Die Daten werden beispielsweise verschlüsselt und mit einer digitalen Signatur gesichert.“ Da aber auch valide Absender bewusst falsche Daten senden könnten, müsse man zusätzlich die Informationen auf ihre Plausibilität und Konsistenz überprüfen.

Kargl berichtet, dass sein Team in einem anderen Projekt an Computersystemen arbeite, die gegen Infektionen durch Schadsoftware immun seien. Aus vielen solcher Bausteine würden sich sichere Computersysteme ergeben.

Hürden einbauen für mehr Sicherheit

Grundsätzlich empfiehlt Kargl, sich nicht auf einzelne Maßnahmen zu verlassen: „Kein Sicherheitsmechanismus ist unüberwindbar. Unser Ziel ist deshalb eine IT-Sicherheit durch in der Tiefe geschachtelte Mechanismen, die für den Angreifer mehrere Hürden darstellen.“ Er beklagt, dass die IT-Sicherheit von einigen Herstellern noch immer nicht ernst genug genommen wird, und vermutet, dass

Andreas Zwißler ist Geschäftsführer der ACD Elektronik GmbH aus Achstetten. Das Unternehmen nimmt die Sicherheit bei der Produktentwicklung sehr ernst.

Foto: Martina Dach

die IT-Sicherheit der Produkte in den Augen der Kunden keinen erkennbaren Mehrwert darstellt, für den sie mehr bezahlen würden. Dabei gehöre die IT-Sicherheit bei elektronischen Systemen zur elementaren Produktqualität.

Produktqualität beinhaltet auch IT-Sicherheit

Diese Ansicht teilt auch Armin Steck, Director Cloud Solutions bei der Diehl Connectivity Solutions GmbH in Wangen. Das Unternehmen ist ein Hard- und Software-Anbieter für die intelligente Vernetzung und systemübergreifende Steuerung von Gebäudetechnik. Entwickelt werden modulare Systeme mit offener Schnittstellenarchitektur, sodass Endgeräte verschiedener Hersteller eingebunden werden können. Die Steuerung erfolgt über eine App mit einheitlicher Bedienoberfläche auf Smartphone, Tablet-PC oder Browser.
Für das Unternehmen steht die System- und Datensicherheit an erster Stelle und in direktem Zusammenhang mit der Produktqualität. Das ist nachvollziehbar, wenn man an die Vorbehalte denkt, die es gegenüber Smart-Home-Lösungen gibt. So manch ein Häuslebauer fürchtet ein Hacken des Systems und die unerlaubte Einflussnahme auf die Haustechnik.
Diehl hat für seine Produkte Vorkehrungen getroffen. Die einzelnen Geräte werden von einem Gateway gesteuert, einer zentralen Steuerungseinheit mit verschiedenen Schnittstellen. Die Kommunikation zwischen Gateway und zum Beispiel Jalousien-Aktor erfolgt über Funksignale.

Keine hundertprozentige Sicherheit

„Wir arbeiten hier mit sicheren Funkstandards wie Z-Wave oder EnOcean“, erläutert Armin Steck das System. „Aber natürlich gibt es keine hundertprozentige Sicherheit. Deshalb sind wir noch einen Schritt weitergegangen. In einem hochsicheren Rechenzentrum in Deutschland betreiben wir ein aus mehreren Sicherheitsstufen aufgebautes Backend-System. Über die App des Nutzers wird über ein digitales Zertifikat Kontakt mit dem Backend aufgenommen. Das Backend prüft, ob der Anfragende zugriffsberechtigt ist. Dann identifiziert es sich beim Gateway und löst die gewünschte Aktion, beispielsweise Licht einschalten, aus. Der Nutzer kann nicht direkt über die App auf die Aktoren im Haus zugreifen.“
Darüber hinaus werde die Sicherheit jedes Produktes durch Penetrationstests geprüft. Dazu würden externe Hacker damit beauftragt, das System zu knacken. Erst wenn die größtmögliche Sicherheit gewährleistet sei, werde ein Produkt verkauft.

Sicherung von personenbezogenen Daten

Ähnliche Vorkehrungen im Hinblick auf die IT-Sicherheit ihrer Software hat die BITE GmbH getroffen. Das Ulmer Unternehmen entwickelt Web-Applikationen im Bereich Bewerbermanagement und ist nach ISO 27001 zertifiziert. Diese Zertifizierung befasst sich mit der Implementierung eines Informationssicherheits-Managementsystems. Geschäftsführer Hubert Ketterer weiß um die sensible Handhabung personenbezogener Daten und stellt zwei Faktoren in den Mittelpunkt: die Organisationssicherheit und die Applikationssicherheit der Software. Die Kommunikation der Software mit dem Server basiert auf einer zertifikatsbasierten Transportverschlüsselung. Auf diese Weise werden auch Onlinebewerberformular und Bewerbermanager gesichert. Die Endnutzer werden durch die Software außerdem zur Vergabe eines sicheren Passwortes nach BSI-Standard gezwungen. Eine Firewall sperrt alle Zugriffe auf unerlaubte Ports. Anfragen auf zulässigen Ports werden an einen Load-Balancer weitergeleitet, der Pfad und URL-Struktur prüft. Die Identität der kommunizierenden Person wird so sichergestellt. Alle Bewerberdaten werden verschlüsselt auf einem gesicherten Server bei der BITE GmbH aufbewahrt.

Foto: Rolf Schultes/Drumlin Photos

Für Armin Steck von der Diehl Connectivity Solutions GmbH steht die System- und Datensicherheit in direktem Zusammenhang mit der Produktqualität.

Hubert Ketterer ist Geschäftsführer der BITE GmbH, die Web-Applikationen in den Bereichen Bewerbermanagement sowie Personalmanagement anbietet.

„Schon bei der Softwarearchitektur achten wir auf sicheres Programmieren mit einem Vier-Augen-Prinzip. Automatische Tests prüfen neue Codes, und für die Nutzung der Daten haben wir ein granulares Rollen- und Benutzerkonzept installiert, welches personifizierte Lese- und Schreibzugriffe innerhalb der Software ermöglicht", beschreibt Ketterer die Sicherheitsmaßnahmen. Bezüglich der Organisationssicherheit verweist er auf die Zertifizierung nach ISO 27001. Darüber hinaus hat die BITE GmbH alle Mitarbeiter und Dienstleister zur Geheimhaltung verpflichtet. Die eigene IT-Infrastruktur wird selbst gewartet, aktualisiert und ist mehrfach abgesichert. Der Serverraum ist mit einer zweistufigen Zugangskontrolle geschützt, wird videoüberwacht und erlaubt nur autorisierten Personen den Zutritt während definierter Zeitfenster. „Unser Ziel ist die kontinuierliche Verbesserung der Software, der Prozesse und der internen Verfahren", so Ketterer. „Wir wollen uns weiterentwickeln und nicht stehen bleiben."

Gefahren früh erkennen

Als regionaler Internetprovider muss sich auch die TeleData GmbH Friedrichshafen den Herausforderungen in puncto IT-Sicherheit stellen. Im Segment Hosting bietet das Unternehmen Internetdienste wie E-Mail, Speicherplatz für Homepages und Domaindienste an. „Wir arbeiten mit Firewalls, Spam-, Viren- und Malware-Erkennung", schildert Geschäftsführer Armin Walter. „Mittels eines Monitoringsystems wird jeder Dienst kontinuierlich überwacht. Gefahren werden durch Analysen von Verhaltensmustern von uns früh erkannt, sodass wir Maßnahmen wie etwa die Einrichtung von Umleitungen für den Datenfluss ergreifen können." Das Hosting findet im eigenen Rechenzentrum statt und ist nach ISO 27001 zertifiziert. Ein Vier-Augen-Prinzip der Administratoren, Alarmsysteme, Zutrittskontrollen, eine Mehrfaktor-Authentifizierung und weitere Features sichern das Rechenzentrum.

Unabhängigkeit vom Internet

Zum Angebot von TeleData gehören auch Cloud- bzw. IaaS-Produkte (Infrastructure as a Service), das heißt, Kunden können ihre Daten dort speichern und verwalten. Die Kundenkommunikation erfolgt über Verschlüsselungen und Authentifizierungen. Besonders sicher wird die Kommunikation durch die Unabhängigkeit vom Internet. Walter erklärt das so: „Wir verfügen über ein eigenes Glasfasernetz im Großraum Bodensee-Hegau-Allgäu. Damit können wir Verbindungen von Netzwerkabschnitt zu Netzwerkabschnitt herstellen, die keinen Störeinflüssen unterliegen. Unsere Kunden bekommen dazu ein Abschlussgerät für eine virtuelle Punkt-zu-Punkt- oder physikalisch direkte Verbindung zwischen Kundenstandort und Rechenzentrum – ohne das Internet zu benutzen. Damit ist das Haupteinfallstor für Cyberkriminelle versperrt." Der Zertifizierung nach ISO 27001 misst Armin Walter große Bedeutung bei: „Sie beweist Professionalität und ist elementar für unseren Verkauf, insbesondere bei Ausschreibungen von Rechenzentrumsflächen."

Gefahr durch Android-System in der industriellen Anwendung

Nicht alle Devices sind für Hacker interessant. Manche davon sammeln einfach nur Daten und liefern sie an Rechenzentren. Die dort erfassten Daten sind ein viel größerer Anreiz zum Datenklau. Deshalb sieht Geschäftsführer Andreas Zwißler die Sicherheit der Produkte der ACD Elektronik GmbH aus Achstetten weniger gefährdet. Und doch sieht er Handlungsbedarf. Das Unternehmen entwickelt und produziert mobile Geräte für Handel und Logistik, industrielle Anwendungen und das Gesundheitswesen. Als Beispiel nennt Zwißler den mobilen Barcodeleser, der in Handel und Lagerverwaltung zum Einsatz kommt. Das Gerät liest den Barcode

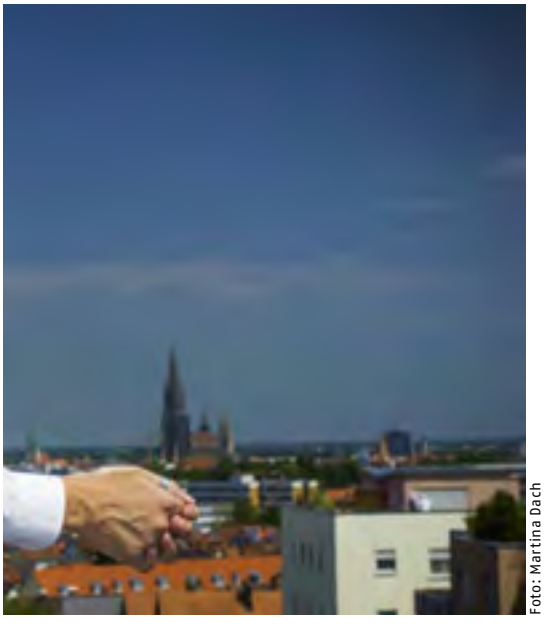

Foto: Martina Dach

Foto: Rolf Schultes/Drumlin Photos

Armin Walter, Geschäftsführer der TeleData GmbH, setzt bei der Sicherheit auch auf die Unabhängigkeit vom Internet.

Foto: Rolf Schultes/Drumlin Photos

Enno Littmann, Geschäftsführer der IHSE GmbH, arbeitet mit KVM-Technologie, die größtmögliche IT-Sicherheit bietet.

ein und funkt die Daten an einen Zentralrechner. Die Funkverbindung kann über ein geschlossenes WLAN-Netz erfolgen oder über Mobilfunk. Der Mobilfunk bietet Angriffsfläche zum Abgreifen von Daten, weshalb eine Verschlüsselung vorgenommen wird. „Die Sicherheit ist Bestandteil unserer Produktentwicklung und wird von uns ernst genommen", erläutert Zwißler. „Eine weit größere Gefahr für Cyberangriffe bieten jedoch die Server unserer Kunden, auf deren Sicherheit wir keinen Einfluss haben. Wir bieten deshalb Penetrationstests an. Dabei prüft ein externes Unternehmen die Geräte und Datenverbindungen auf Schwachstellen." Auch wenn seine Geräte kaum Gefahr laufen, gehackt zu werden, sieht Zwißler neue Gefahren für die Zukunft. „Durch die zunehmende Vernetzung der Industrie wird der Cyberkriminalität eine breite Angriffsfläche geboten." Dazu trage auch das verbreitete Windows-Betriebssystem bei und der Einzug des bislang auf die Consumer-Welt beschränkten Android-Betriebssystems in industrielle Anwendungen.

Netzunabhängige Profitechnologie

Eine nahezu hundertprozentige IT-Sicherheit strebt die IHSE GmbH in Oberteuringen an. Das Unternehmen ist Weltmarktführer im Bereich KVM-Produkte. KVM bezeichnet Keyboard, Video, Mouse. KVM-Extender ermöglichen die räumliche Trennung von Computern und Arbeitsplätzen über größere Entfernungen und finden ihren Einsatz in Polizei-, Feuerwehr- und Verkehrsleitstellen, in den Towern von Flughäfen, in Kraftwerken, an der Börse sowie in Entwicklungsabteilungen von Konzernen. Kurz gesagt überall dort, wo höchste Sicherheit gefordert ist und kein Rechner direkt am Arbeitsplatz stehen sollte, man aber auf mehrere Bildschirme und Rechner gleichzeitig zugreifen muss. Das System besteht aus einem KVM-Sender und einem -Empfänger, die über Kabel miteinander und mit dem Rechner verbunden sind. Die Datenströme werden verlustfrei komprimiert und ohne spürbare Latenz in Echtzeit übertragen. Die Systemarchitektur ist deshalb hoch sicher, weil nur eine interne Verbindung besteht und keine Funk- oder Internetverbindung. Die Daten werden zuerst codiert und dann übertragen. Ein Matrixswitch ermöglicht es verschiedenen Nutzern, auf verschiedene Rechner zuzugreifen und so miteinander zu arbeiten. Geschäftsführer Enno Littmann erklärt: „Die KVM-Technologie ist eine Schlüsseltechnologie, die größtmögliche IT-Sicherheit bietet. Aber unsere Technik etabliert sich nur langsam im IT-Bereich und ist dort im Gegensatz zu anderen Branchen noch wenig verbreitet. Deshalb engagieren wir uns dafür, auch Studierenden das Wissen um die KVM-Technologie zu vermitteln."

* Birgit Mann ist Wirtschaftsingenieurin Kommunikationstechnik und Inhaberin der Team-Entlastung PR Blaubeuren.

Datenklau, Spionage, Sabotage: zwei Drittel der Industrie betroffen

Grafik: Bitkom

Die Industrie ist betroffen: Der Diebstahl von elektronischen Dokumenten bzw. Informationen rangiert auf Platz 3 der Delikte.

IHK-Ansprechpartner

Kompetente Beratung

Die IHKs Bodensee-Oberschwaben und Ulm beraten umfassend zum Thema Digitalisierung und IT-Sicherheit.

► Info:
IHK Bodensee-Oberschwaben,
Sönke Voss, Tel. 0751 / 409-137,
voss@weingarten.ihk.de
IHK Ulm,
Gernot Schnaubelt, Tel. 0731 / 173-179,
schnaubelt@ulm.ihk.de