Tickende Zeitbombe IoT: Wie Unternehmen ihre vernetzte Infrastruktur sichern, bevor es zu spät ist

Ob Produktionsanlagen, Logistiksysteme, Gebäudesteuerung oder moderne Büroausstattung, Unternehmen aller Branchen setzen seit langem auf IoT-Technologie, um Effizienz und Innovation zu steigern. Doch wo Sensoren, Kameras, Steuerungen und Gateways Einzug halten, bestehen massive Risiken. Die Realität: Viele dieser Geräte wurden nie mit Blick auf Sicherheit entwickelt. Es fehlt an Updates, Authentifizierung, Verschlüsselung. Die Folge: eine riesige, schwer kontrollierbare Angriffsfläche. Doch es gibt Abhilfe.

Es ist 3 Uhr morgens im Unternehmen, Ruhe im Haus. Nur das leise Surren eine IoT-Kamera in der Produktionshalle. Doch auf der anderen Seite dieser Verbindung sitzt kein Techniker, sondern ein Angreifer. Eine 0-Day-Schwachstelle – und schon wird das Gerät zum Einfallstor. Von hier aus kann lateral ins Netzwerk vorgedrungen werden, Daten abfließen oder Systeme verschlüsselt werden. Ein harmloses Gerät wird zur tickenden Zeitbombe.

Ein Szenario, wie wir es als IT-Security-Beratungshaus schon vergleichbar erlebt haben. Und weil niemand Zeitbomben im eigenen System möchte, wird es Zeit für einen Paradigmenwechsel. Weg von punktuellen Patches und "Firewalls als Allheilmittel". Hin zu einem strukturierten, ganzheitlichen Sicherheitsansatz, der die Schwachstelle IoT-Systeme vollumfänglich adressiert.

IoT-Angriffsszenarien: die Gefahr ist real

Dass IoT-Komponenten nicht nur theoretisch, sondern praktisch ein hohes Risiko darstellen, zeigen zahlreiche Vorfälle:

- **Mirai-Botnetz (2016):** Millionen IoT-Geräte wurden zu einer Armee für DDoS-Attacken umfunktioniert, weil deren Standardpasswörter nie ersetzt wurden.
- **Verkada-Hack (2021):** Hacker erhielten Zugriff auf 150.000 Überwachungskameras in Kliniken, Gefängnissen und Unternehmen.
- **Colonial Pipeline (2021):** Ein einzelner kompromittierter Zugang legte die größte Benzin-Pipeline der USA lahm.

Die Angreifer reichen dabei von klassischen Cyberkriminellen bis hin zu staatlich gesponserten Hacker-Gruppen, die gezielt Unternehmen ins Visier nehmen, um sie und damit das ganze Unternehmen zu schädigen. Oft ist nicht das einzelne Gerät das Ziel, sondern das Netzwerk dahinter.

Herausforderungen bei der Absicherung von IoT-Systemen

IoT-Systeme stellen Sicherheitsverantwortliche vor völlig neue Probleme:

1. Heterogenität: Unterschiedliche Hersteller, eigene Protokolle, proprietäre Software.

2. Lange Lebenszyklen: Geräte sind teils über 10 Jahre im Einsatz – ohne Update-Möglichkeit.
3. Limitierte Ressourcen: Geringe Rechenleistung, kein Platz für klassische AV-Software.
4. Verfügbarkeit vs. Sicherheit: Systeme dürfen nicht einfach neugestartet oder aktualisiert werden.
5. Mangel an Transparenz: Oft weiß niemand genau, welche IoT-Geräte im Netz hängen.
6. Keine Wartung der Hersteller mehr: Vieles läuft noch auf Windows 7 und es gibt keine Upgrades.

Die Folge: Die klassischen IT-Sicherheitskonzepte greifen hier nicht oder nur bedingt.

Die vier Säulen eines praxisorientierten Sicherheitskonzepts

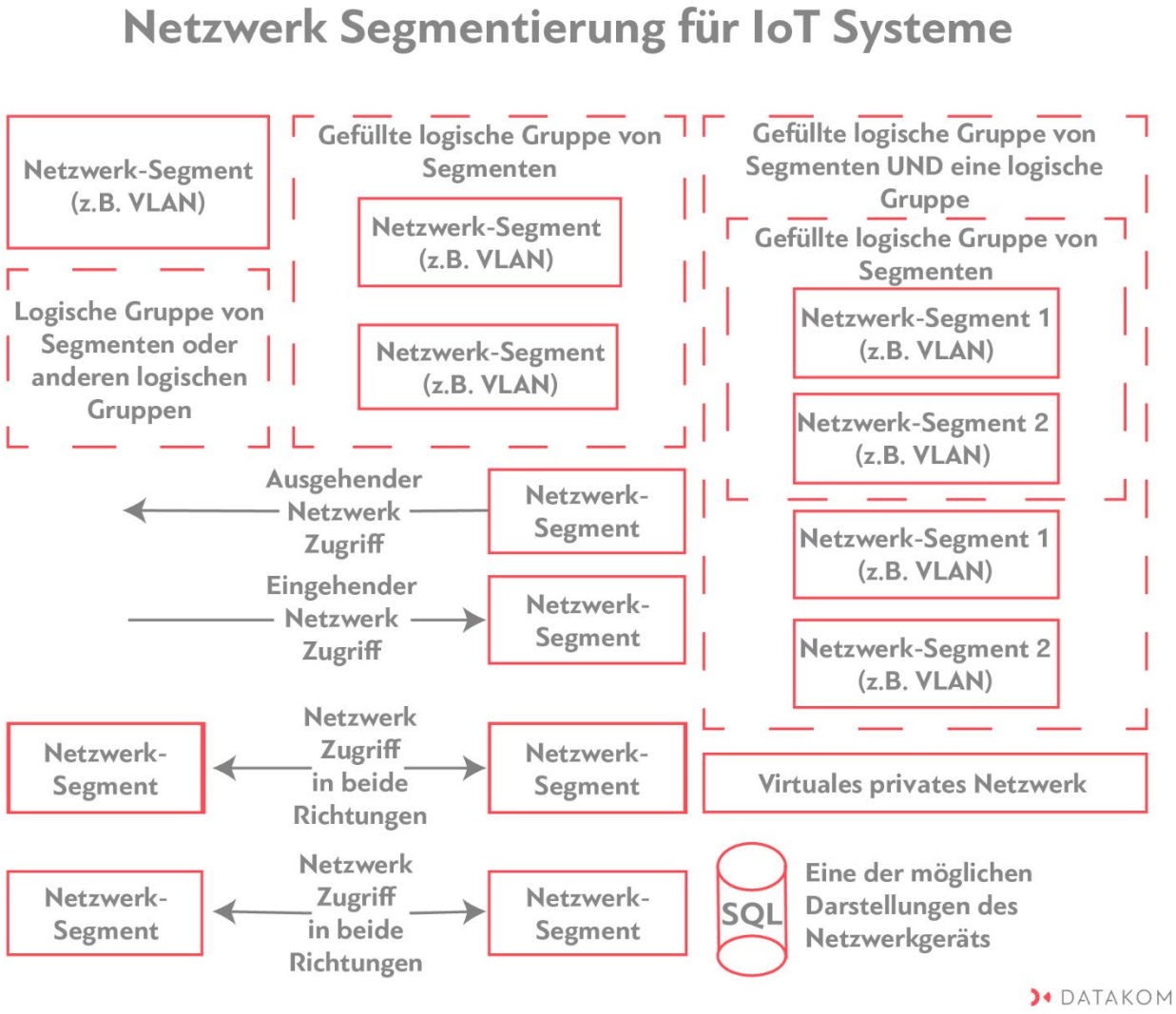
Organisatorische Schutzmaßnahmen

Neben technischen Lösungen sind klare Zuständigkeiten und Prozesse essenziell:

- **Verantwortlichkeiten und Governance:** Bündelung der IoT-Sicherheit unter einem CISO oder einer vergleichbaren Führungsebene, damit IT- und OT-Teams eng zusammenarbeiten. Eine gemeinsame IT/IoT-Governance verhindert Silobildung.
- **Asset-Inventar & Risikomanagement:** Erstellung eines vollständigen Inventars aller vernetzten Systeme, damit ein systematisches Risikomanagement (z. B. im Rahmen eines ISMS) möglich ist.
- **Supply-Chain-Security:** Prüfung und Kontrolle von Drittanbietern, insbesondere bei IoT-Komponenten. Verträge müssen Mindestanforderungen erfüllen.
- **Sicherheitsrichtlinien und Trainings:** Definition verbindlicher Policies (z. B. Passwortregeln, Updatezyklen, Zugangskontrollen) für vernetzte Geräte, flankiert von gezielten Awareness-Trainings für alle Mitarbeitenden.
- **Regelmäßige Audits und Reviews:** Sicherheitsüberprüfungen mit internen wie externen Experten (Penetrationstests, Red Teaming) erhöhen die Reife und das Vertrauen.
- **Incident Response & Notfallplanung:** Entwicklung konkreter Notfall- und Wiederanlaufpläne für IoT-Szenarien sowie regelmäßiges Üben von Vorfällen.
- **Erstellung eines Absicherungskonzepts:** 1) Was wird gekapselt? 2) Was wird geupdatet? 3) Was wird segmentiert?

Technische Schutzmaßnahmen

Praxisnahe technische Lösungen für vernetzte Geräte umfassen unter anderem:



- **Netzwerksegmentierung:** IoT-Systeme gehören in strikt getrennte Netzsegmente – isoliert vom Office- oder Internetbereich.
- **Zero Trust für Maschinenkommunikation:** Keine impliziten Vertrauensstellungen. Kommunikation nur nach dem Prinzip des geringsten Privilegs.
- **Gerätehärtung (Hardening):** Unnötige Dienste deaktivieren, starke Authentifizierung (z. B. Zertifikate). Security by Design und Default werden regulatorisch gefordert.
- **Patch-Management trotz Einschränkungen:** Firmware aktuell halten. Wo nicht möglich, müssen kompensierende Maßnahmen greifen.
- **Anomaliedetektion & Monitoring:** IoT-IDS/IPS analysieren Netzwerkverkehr. Tools wie Suricata, Nozomi oder Wallix bieten moderne Monitoring- und Sicherheitsfunktionen.

- **Absicherung von Fernzugriffen:** Fernzugänge nur über kontrollierte Kanäle – mit MFA, Protokollierung und zeitlicher Begrenzung.
- **Verschlüsselung:** Daten im Transit und bei Bedarf im Ruhezustand verschlüsseln.

Standards und regulatorische Rahmenwerke

Neben organisatorischen und technischen Maßnahmen kann es helfen, wenn Unternehmen sich an bestimmten Standards oder Rahmenwerken orientieren. Diese wurden erarbeitet, um Angriffe auf Unternehmen und auch speziell IoT zu verhindern.

- **ISO/IEC 27001:** Fundament für ein integriertes Managementsystem – auch für IoT.
- **NIST CSF:** Flexibles Framework zur Einordnung und Priorisierung von Schutzmaßnahmen.
- **MITRE ATT&CK for ICS:** Realweltliche Angriffsmodelle zur Verbesserung von Detection & Response.
- **EU-Vorgaben:** NIS2, Cyber Resilience Act u. a. bringen verbindliche Anforderungen für Betreiber und Hersteller.

Technologischer Werkzeugkasten

Sich zu organisieren, und sich durch technische Maßnahmen wie Segmentierungen und ähnliches zu schützen, ist elementar. Auf technologischer Seite gibt es jedoch auch viel Hilfe, damit die eigene IoT nicht zum Einfallstor für Hacker wird.

- **Asset Discovery:** z. B. Nmap, Fing, Advanced IP Scanner
- **Vulnerability-Scanner:** Tenable Nessus, OpenVAS
- **IoT-Security-Plattformen:** Tenable.ot, Nozomi, Claroty
- **Firewall/IDS/IPS:** FortiGate, Palo Alto, Suricata
- **Update-Management:** Puppet, Ansible, Mender
- **Zero-Trust-Zugriff:** ZTNA-Plattformen, VPN-Gateways mit PKI & TPM
- **Privileged Access Management (PAM):** z. B. Wallix OT Security mit Session-Überwachung und rollenbasierten Zugriffen

Fazit: Jetzt handeln, nicht später patchen

Die Risiken sind real, die Bedrohungen aktiv, und der Schutz vieler Unternehmensnetzwerke unzureichend. IoT-Sicherheit ist kein Nice-to-have, sondern eine Grundvoraussetzung für Resilienz. Ein Satz, den wir unseren Kunden immer wieder ans Herz legen: Wer heute nicht handelt, setzt morgen Daten, Geschäftsprozesse, Reputation und vielleicht sein ganzes Unternehmen aufs Spiel.

Der Weg ist nicht einfach, aber klar: Mehrschichtige Sicherheitsarchitektur, Zero Trust als Leitprinzip und ein durchdachter Lifecycle-Ansatz sind der Schlüssel zu robusten IoT-Systemen und deren Governance. Die Zeit zu handeln ist jetzt. Denn erfolgreiche Angriffe auf die IoT können verheerende Auswirkungen haben.