



Link: <https://www.cio.de/a/sechs-schritte-zum-sicheren-iot,3259838>

Security-Strategie

Sechs Schritte zum sicheren IoT

Datum: 13.07.2016

Das IoT stellt auf Grund der vielen vernetzten Geräte und Daten hohe Anforderungen an die Sicherheit. CIOs müssen umgehend eine umfassende Security-Strategie entwerfen.

Rund 28 Milliarden Geräte und Sensoren werden laut einer **Prognose von IDC¹** im Jahr 2020 das Internet der Dinge bilden. Dabei wird der Großteil der "Dinge" professionellen Lösungen entstammen, mit denen Unternehmen beispielsweise Daten über Produkte sammeln, Fertigungsabläufe steuern und optimieren sowie Unternehmensprozesse beschleunigen wollen.

Für die Unternehmen ist **laut Matthias Röse²**, IoT Strategist EMEA bei Hewlett Packard Enterprise (HPE), eine der Herausforderungen, "die großen Datenmengen miteinander so zu verknüpfen, dass sie im Geschäftsbetrieb nutzbar gemacht werden können". **Ins gleiche Horn³** stößt auch Nik Rouda, Senior Analyst bei The Enterprise Strategy Group (ESG). **In einem Whitepaper schreibt er: "Die Dinge sind nur Mittel zum Zweck, um Daten zu erfassen oder in manchen Fällen auch die Systeme zu steuern." Das restliche System müsse auf die wirkungsvolle und sichere Verwendung der Daten ausgerichtet werden.⁴**

Sicherheit wird beim IoT noch häufig vernachlässigt

Dazu gehört nicht nur die Installation der geeigneten **Infrastruktur⁵** zum Transport der Datenflut, sondern insbesondere auch der Aufbau einer widerstandsfähigen Sicherheitsumgebung für das Internet der Dinge. "In einer hochvernetzten Welt, in der alles mit allem kommuniziert, lassen sich Identitäten schwer rückverfolgen", **sagt Andrzej Kawalec⁶**, HPE Chief Technology Officer, Security Services. "Wegen der Geräte, die außerhalb des klassischen Perimeterschutzes installiert sind, vergrößert das IoT die Angriffsfläche dramatisch." Hinzu kommt, dass bei vielen Geräten Sicherheitsaspekte bei der Entwicklung nicht ausreichend berücksichtigt wurden und diese deshalb häufig Sicherheitslücken aufweisen.

Eine kürzlich veröffentlichte **Untersuchung der Economist Intelligence Unit⁷** weist in diesem Zusammenhang darauf hin, dass sich die großen Unternehmen auf der einen Seite intensiv mit dem Internet der Dinge auseinandersetzen und neue Geschäftsmodelle schaffen würden. Auf der anderen Seite blenden die C-Level-Manager und die Geschäftsführung aber die Datensicherheit völlig aus.

Umfassende Sicherheitsstrategie implementieren

Das ist eine gefährliche Entwicklung, die aufgehalten werden muss - unabhängig von den Budgetzwängen der IT-Abteilungen. Sie müssen schnellsten Kompetenzen aufbauen, um sowohl mit der technischen Entwicklung als auch mit der Sicherheitsproblematik Schritt zu halten.

Ohne ein umfassendes Sicherheitskonzept, das alle Bereiche des Unternehmens umfasst, setzen sich die Unternehmen unkalkulierbaren Risiken aus. Die Economist-Analysten weisen überdies darauf hin, dass in vielen Unternehmen IoT-Initiativen dezentral in den Unternehmensbereichen entstanden sind, die nun möglichst schnell in eine effektive, einheitliche Sicherheitsstrategie eingepasst werden müssen. "Sind die Lösungen erst einmal in Betrieb, dann kann es extrem schwierig werden, tausende von Geräten sicherheitstechnisch umzurüsten", schreiben sie im Whitepaper.

Externe Partner sorgen für Know-how

Fraglich ist, ob die IT-Teams der Unternehmen diese Herkulesaufgabe selbst bewältigen können. Immerhin stellte der "**Cyber Risk Report 2016**" von HPE⁸ fest, dass 86 Prozent der Firmen nicht über die notwendigen Security-Fähigkeiten und -Kenntnisse verfügen, um den aktuellen Bedrohungen für die IT-Sicherheit zu begegnen.

Eine zu dünne Personaldecke oder fehlende Kompetenzen dürfen aber nicht als Ausrede für die unzureichende Beschäftigung mit der IoT-Sicherheit herhalten. **HPE-CTO Andrzej Kawalec empfiehlt**⁹ vielmehr den Unternehmen, einen oder mehrere Partner mit der notwendigen Security-Kompetenz ins Boot zu holen. Das ist auch im Hinblick auf Ergebnisse des "**M-Trends 2016 Report**"¹⁰ von Mandiant sinnvoll. Dieser offenbart, dass nur wenige Fälle, um die sich die Sicherheitsexperten von Mandiant im vergangenen Jahr kümmern mussten, von den Unternehmen selbst entdeckt wurden.

6 Schritte zum sicheren IoT

Als Schlussfolgerung ihrer Studie empfehlen die Analysten von The Economist Intelligence Unit den Unternehmen sechs Schritte für eine sichere Nutzung des Internet der Dinge:

1. Einführung einer umfassenden Strategie für digitale Sicherheit

Klassische, reaktiv arbeitende Perimeter-Schutzsysteme wie Firewalls oder Intrusion-Detection-Systeme sind den heutigen Cyberbedrohungen alleine nicht mehr gewachsen. Unternehmen benötigen ein proaktives, unternehmensweites Sicherheitskonzept, das auf die Sicherheit des IoT abgestimmt ist. Dafür ist die Unterstützung des CEO und der Geschäftsführung nötig.

2. Umfassendes Audit der aller IoT-Projekte

Für die bestmögliche Sicherheit sollten Unternehmen alle vorhandenen und geplanten Installationen und Projekte mit speziellem Fokus auf eventuelle Sicherheitsschwachstellen bewerten. Dabei darf man sich nicht auf die IoT-Geräte beschränken, sondern muss auch die Netzwerkinfrastruktur, alle Mobilgeräte und Cloudlösungen einbeziehen.

3. Frühzeitige Implementierung von Sicherheitsmaßnahmen

Unternehmen sollten nicht den Fehler begehen, sich erst nach der Installation der IoT-Geräte um deren Sicherheit zu kümmern. Sicherheit sollte von Anfang an Teil des Projektes sein - bei der Entwicklung neuer Geräte, bei der Erweiterung der IT-Infrastruktur, bei der Integration neuer Dienstleistungen.

4. Sensibilisierung der Mitarbeiter für IoT-Sicherheitsthemen

IoT ist kein reines IT-Projekt. IoT wirkt bis tief in das Produktdesign, die Lieferkette, die Fertigung und andere Unternehmensprozesse hinein. Alle damit befassten Mitarbeiter müssen in das Sicherheitskonzept einbezogen werden.

5. Partner müssen Teil des Sicherheitskonzepts sein

Auch bei IoT bestimmt das schwächste Glied das Sicherheitsniveau der ganzen Umgebung. Deshalb müssen Unternehmen sicherstellen, dass alle Partner (Kunden, Lieferanten, externe Partner, etc.) den gleichen strengen Sicherheitsvorgaben folgen wie das Unternehmen selbst.

6. Überdenken Sie die Rolle der IT

Mit dem Internet der Dinge ändert sich die Rolle der IT-Abteilung grundlegend. Sie ist nicht länger bloßer Dienstleister, sondern Partner in nahezu allen Unternehmensabläufen. Dafür müssen Organisationsstrukturen verändert, neue Kompetenzen geschaffen und andere Hierarchien implementiert werden.

Links im Artikel:

¹ <http://w.idg.de/29uVJgC>

² <http://w.idg.de/29H01pC>

³ <http://w.idg.de/29uVJgC>

⁴ <http://w.idg.de/29HLYS6>

⁵ <http://w.idg.de/29CHk67>

⁶ <http://w.idg.de/29rbVEI>

⁷ <http://w.idg.de/29xOdCC>

⁸ <http://w.idg.de/29sjkdH>

⁹ <https://www.youtube.com/watch?v=V0JPQ5F4DrA>

¹⁰ https://www.fireeye.com/blog/executive-perspective/2016/02/m-trends_2016.html

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.