Mittelstand 4.0
Kompetenzzentrum
Cottbus

FACHBROSCHÜRE

INTERNET DER DINGE – INTERNET OF THINGS (IOT)

Herausforderung IT-Sicherheit

www.kompetenzzentrum-cottbus.digital

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IMPRESSUM

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Cottbus
c/o Technische Hochschule Wildau
Hochschulring 1
15745 Wildau
Tel.: +49 3375 508782

Vertreten durch: Die Technische Hochschule Wildau ist eine Körperschaft des öffentlichen Rechts. Sie wird nach außen durch die Präsidentin, Prof. Dr. Ulrike Tippe, vertreten.

Zuständige Aufsichtsbehörde: Die Hochschule untersteht der Rechtsaufsicht des Ministeriums für Wissenschaft, Forschung und Kultur des Landes Brandenburg.

Autoren:
Jan Seitz, Sabrina Quaal, Alexander Dietrich

Satz/Layout:
maerkbar – Cottbus

Bildnachweis:
Umschlag: Darwin Laganzon – Pixabay
Seite 3: Jordan Harrison – Unsplash
Seite 5: Boskampi – Pixabay
Seite 8: Andre Taissin – Unsplash
Seite 11: Eigene Dartstellung
Seite 12: Fotos Alexander Dietrich

Vorbemerkung: Was ist das Internet der Dinge?

Die Heizung per Fernzugriff von Unterwegs einschalten, den Saugroboter per App steuern oder die Kaffeemaschine mit dem Wecker vernetzen: Das Internet der Dinge (engl. Internet oft Things, Abk.: IoT) erleichtert uns das Leben. Doch nicht nur privat. Auch die Industrie profitiert von „intelligenten“ und vernetzten Anwendungen. Smarte Produktionen sparen Energie, Zeit und Kosten. Möglich wird dies, weil das IoT die reale mit der virtuellen Welt verbindet. **Dazu werden „Dinge“** – in Unternehmen etwa Videokameras, Maschinensteuerungen oder Waren im Lager – **mit kleinen Chips, Datenspeichern oder Softwaresystemen ausgestattet und über das Internet miteinander vernetzt.** Dadurch kann jedes „Ding Informationen bereitstellen und mit anderen vernetzten „Dingen“ kommunizieren. Das IoT macht viele Anwendungen möglich, z. B. per App steuerbare Saugroboter, smarte Toaster, selbstständig bestellende Kühlschränke, automatische Klimatisierung oder vernetzte Straßenlaternen. Es ist auch ausschlaggebend für neue Möglichkeiten der Industrie 4.0, Smart-City-Anwendungen oder e-Health. Im Einsatz bei Unternehmen der Industrie wird oft vom **„Industrial Internet of Things“ (IIoT)** gesprochen, dessen Fokus z. B. sich selbst steuernde und organisierende Förderanlagen sind. Typische Anwendungsfälle für (I)IoT-Lösungen liegen z. B. in der Automatisierung, Koordination, Dokumentation oder Remote-Steuerung von Anlagen. Dadurch lassen sich Produktionsketten effizienter und effektiver einstellen und neue Geschäfts- und Servicemodelle werden möglich. Einen tieferen Einblick finden Sie hierzu in der Fachbroschüre **„Internet der Dinge (Internet of Things) – Grundlagen, Anwendungsbereiche, Potenziale“**.

Dieser großen bunten Welt der Möglichkeiten und Potenziale stehen aber auch Herausforderungen gegenüber. Sie sind etwa in der Produktauswahl, der Implementierung oder der konkreten Prozessintegration, insbesondere jedoch im Bereich der IT-Sicherheit zu finden, da IoT-Lösungen zwangsläufig verschiedene Systeme miteinander vernetzen. Diese Fachbroschüre thematisiert daher die allgemeine Situation, typische Stolpersteine und mögliche Lösungsansätze für die Erhöhung der IT-Sicherheit im Zusammenhang mit IoT-Lösungen.

Hier geht es zur Fachbroschüre

www.kompetenzzentrum-cottbus.digital/Media/public/Website/Upload/Broschuere_IoT.pdf

Sicherheitsherausforderungen in vernetzten Systemen

Moderne Systeme sind in der Regel ganz oder teilweise softwaregetrieben, rein mechanische Komponenten werden immer seltener. Mit dem Ansatz, alles „smarter“, also intelligenter zu machen, werden Alltagsgegenstände mittels Sensoren programmiert und über das Internet vernetzt. Längst haben viele Akteure erkannt, dass die Nutzung von (Echtzeit-) Daten erhebliche Potenziale aufweist. So gibt es zum Beispiel smarte Bohrmaschinen, welche sich über eine App einstellen lassen und das notwendige Drehmoment für ein „optimales Bohr- oder Schraubergebnis“ automatisch bestimmen. Auch die zentrale Fernsteuerung von Geräten und Anlagen, z.B. im Bereich des Smart Home, stößt derzeit auf großes Interesse. Solche Systeme sind jedoch **grundsätzlich anfällig für (un-)absichtliche Konstruktions- und Programmierfehler**, die Sicherheitslücken mit sich bringen und die Nutzenden angreifbar machen. Solche Sicherheitslücken lassen sich oft auch bei höchster Sorgfalt nicht vermeiden, wie später noch ausgeführt wird. Die Nutzung von modernen Systemen, z. B. von smarten Geräten, ist deshalb grundsätzlich mit Risiken verbunden.

Dies gilt umso mehr, da diese Systeme in aller Regel **vernetzt**, überwiegend sogar mit **Internetzugang** ausgestattet sind. Das wird insbesondere dann ein Problem, wenn die Systeme z. B. in das Firmennetzwerk eingebunden sind. Angreifer müssen sich dann mitunter gar nicht durch diverse Sicherheitsbarrieren (z. B. Firewall) durchkämpfen, sondern können über einzelne schlecht oder nicht ausreichend gesicherte Geräte eindringen. Bereits vor einigen Jahren gab es die ersten Vorfälle von gehackten Kühlschränken und Kaffeemaschinen, über die in Netzwerke eingedrungen wurde. **Wann wird die smarte Bohrmaschine zum Einfallstor – oder ist sie es bereits?**

Viele Unternehmen investieren in ihre IT-Sicherheit. Da dürfte die Gefahr eines Hacker-Angriffs über IoT-Geräte, wie den smarten Kühlschrank, eher eine Gefahr für Privatpersonen sein? Ein Blick in die Praxis zeigt jedoch, dass es auch bei Unternehmen zu großen Sicherheitslücken kommen kann: Wie viele Unternehmen kennen sämtliche in ihrem Netzwerk aktiven Geräte und überwachen diese ständig? Tatsächlich sind die möglichen Einfallstore gar nicht bekannt. „Hand auf‘s Herz“ – wie steht es in Ihrem Unternehmen? Ist IT-Sicherheit vollständig beherrscht oder sind eher Verbesserungen notwendig?

Einfallstore gibt es auf Grund der Digitalisierung immer mehr, aus denen sich die Notwendigkeit entsprechender Maßnahmen ableitet. Vielen Unternehmen ist dabei nicht bewusst, wie attraktiv sie für mögliche Angreifer sein können. Auch ein Unternehmen ohne eigene Entwicklungsabteilung, kann aufgrund von Kundendaten einen Angriff interessant machen, wenn er aufwandsarm durchgeführt werden kann. Auch die Verschlüsselung von Daten zur Erpressung von Lösegeldern kann selbst bei kleinen Unternehmen lukrativ sein. Zudem sind Kollateralschäden nicht unüblich, wenn z. B. Viren oder Trojaner ganz „herkömmlich“ eindringen, ohne dass das Unternehmen wirklich gezielt angegriffen worden wäre.

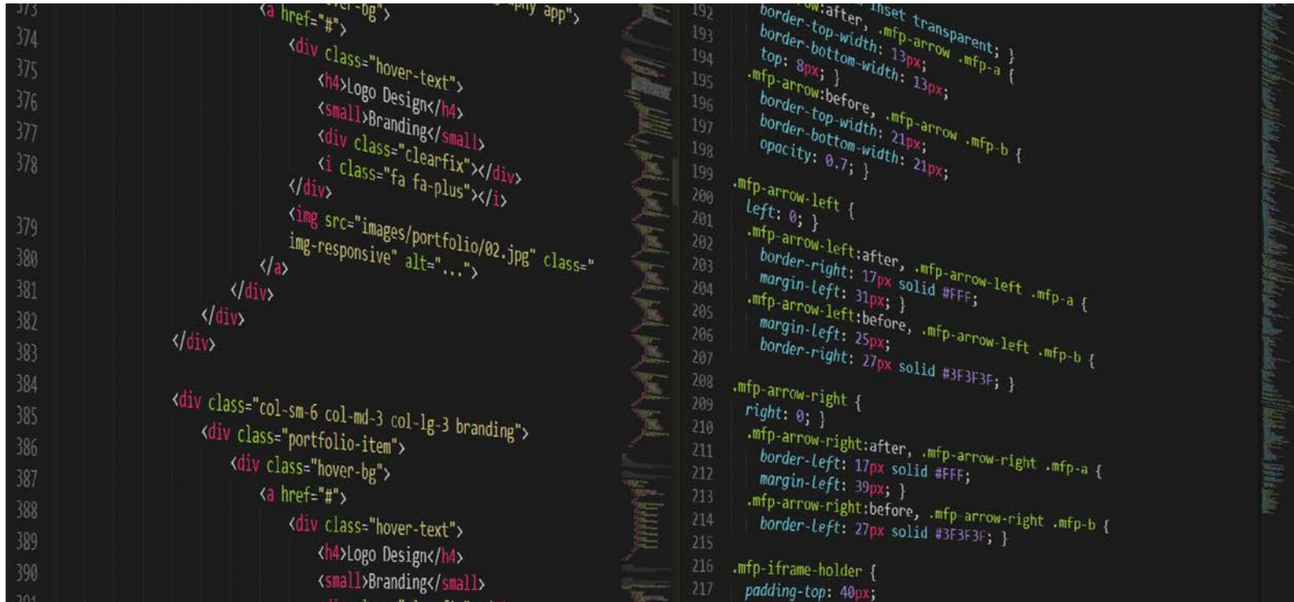
Die Verhinderung solcher Vorfälle stellt alle Akteure von Kleinst- bis Großunternehmen vor eine Herausforderung. Die Dynamik ist hoch, die IT-Sicherheit muss dem technologischen Fortschritt angepasst werden. Nicht jedes Unternehmen hat hierfür die nötigen Fachkräfte und Ressourcen. Aber selbst mit ausreichend Fachkräften und Ressourcen ist die Verhinderung von Sicherheitsproblemen in vernetzten Systemen immer ein Wettlauf gegen die Zeit und gegen Unbekannt – gegen unbekannte Angreifer und (in der Regel) unbekannte Sicherheitslücken.

Sicherheitslücken

Nach Harry Sneed, einem Pionier der Software-Testtechnologie, stecken in 1.000 Zeilen Programmcode durchschnittlich 7 Programmierfehler, wobei die Bandbreite von 0,2 Fehlern in sicherheitskritischer Software (z. B. militärische Systeme) bis zu 18 Fehlern in Webapplikationen, auf die der Webbrowser zugreift (z. B. Webmail oder Online-Shops) reicht. Diese Programmierfehler entstehen aus menschlichen Fehlern ganz natürlich in der Programmierung und werden bei Tests oft nicht entdeckt, wenn sie nicht wesentliche Fehlfunktionen verursachen.

Nimmt man nun Windows 10 mit geschätzten 50 Millionen Codezeilen, dann sind in diesem Code – die durchschnittlichen 7 Fehler je 1.000 Zeilen Code angenommen – 350.000 Fehler verborgen. Hinzu kommen in der Regel Gerätetreiber, spezialisierte Software und auch weitere Komponenten mit eigenen Codes, sodass die Gesamtzahl der notwendigen Codezeilen für einen gegebenen Anwendungsfall (z. B. Aufnahme eines Videos über eine fest installierte Kamera, Verarbeitung auf einem Windows-Rechner und Speicherung in einer Datenbank) problemlos 100 Millionen überschreiten kann – mit entsprechendem Fehlerpotenzial. Software ist somit per se unsicher, zumal sie in der Regel nie „fertig“ ist, sondern immer wieder aktualisiert und erweitert wird, oft auch mit „Add-Ons“ oder „Plug-Ins“ von Drittanbietern, die wiederum neue Fehler mitbringen können.

Natürlich schließen die meisten Hersteller mit „Updates“ (Aktualisierungen) und „Patches“ (Fehlerbehebungen) regelmäßig



Lücken und beheben Probleme, eine „fehlerfreie“ oder „lückenlose“ Software ist auf absehbare Zeit aber ein Wunschtraum. Sicherheitslücken können zudem durch die Verwendung von Software für nicht-vorgesehene Zwecke entstehen oder wenn beispielsweise Software genutzt wird, die keine Aktualisierungen mehr erhält (z. B. Windows XP, welches immer noch auf mehr als einem Prozent aller Rechnersysteme weltweit genutzt wird, u. a. auch in Anlagensteuerungen und Industrieanlagen, obwohl es seit dem 08.04.2014 nicht mehr von Microsoft unterstützt wird).

Nicht alle Sicherheitslücken sind ein Sicherheitsproblem. Allerdings sind Fehler, die die Ausführung von Schadcode erlauben, kritisch. Sicherheitslücken werden entweder zufällig durch Anwender gefunden, durch gezielte Suche Dritter aufgedeckt oder automatisch identifiziert, z. B. von Codecheckern – Anwendungen, die Programmcode auf Fehler hin untersuchen. Sie werden entweder geheim gehalten oder veröffentlicht, woraufhin Hersteller in der Regel Sicherheitsupdates bereitstellen. Diese müssen jedoch noch installiert werden, was nicht alle Unternehmen zeitnah realisieren (können). Generell können viele Sicherheitslücken auch extern adressiert werden (z. B. durch Vorschaltung einer Firewall und der gezielten Blockierung einzelner Ports), zuverlässiger ist aber die Schließung der Lücke. Sicherheitslücken werden in der IT-Branche kaum thematisiert. Dabei ist die Zahl von IT-Angriffen nicht zu unterschätzen. Auch Hardware-Schwachstellen wie Intels „Spectre“ und „Meltdown“ beschäftigen uns noch heute.

Weitere Informationen zu Sicherheitslücken:

Ein Überblick zur Fehlerhäufigkeit in Programmcode
http://greiterweb.de/spw/Software-Fehler-Dichte.htm

Der Flughafen BER nutzt stellenweise noch Windows XP
https://www.zdnet.de/88388405/19-jahre-windows-xp-kein-glueckwunsch/

Übersichtsartikel zum Umgang mit Sicherheitslücken
https://www.heise.de/ct/artikel/Vom-Umgang-mit-Sicherheitsluecken-4537895.html

BSI verschweigt jahrelang Sicherheitslücken in TrueCrypt
https://www.golem.de/news/verschluesselungssoftware-bsi-verschweigt-truecrypt-sicherheitsprobleme-1912-145486.html

E-Mail kann iPhone oder iPad übernehmen, kein Patch verfügbar
https://www.mactechnews.de/news/article/Vollzugriff-E-Mail-kann-iPhone-und-iPad-uebernehmen-kein-Patch-verfuegbar-174883.html

Analyse: Meltdown und Spectre sind ein Security-Supergau
https://www.heise.de/security/meldung/Analyse-zur-Prozessorluecke-Meltdown-und-Spectre-sind-ein-Security-Supergau-3935124.html

Stellenwert von Sicherheit?

Wenn Sicherheitslücken nicht vermeidbar sind – wie gehen wir dann mit dem Thema Sicherheit und Schutz in unseren Netzwerken um? Welchen Stellenwert hat die Sicherheit? Diese Frage muss jedes Unternehmen für sich selbst beantworten. Einige der üblichen Aspekte hierbei sind die folgenden:

- **Sicherheit ist ein Kostenfaktor:** Sicherheit kostet Geld. Sicherheitsfunktionen zu entwickeln, zu implementieren, zu testen und dauerhaft aktuell zu halten erfordert beim Hersteller erhebliche Ressourcen, die sich im Produkt- und / oder Supportpreis niederschlagen. Oft werden fertige Standardkomponenten (etwa Kommunikationsprotokolle) genutzt, sodass Fehler in diesen Komponenten mehrere Millionen Geräte betreffen können. Zudem ist Sicherheit häufig ein nachgelagerter Schritt und nicht integraler Bestandteil der Produktentwicklung, mit negativen Folgen für die Wirksamkeit. Sicherheit „by design“ ist unüblich. Geradezu sträflich sind die häufigen Fälle, in denen verfügbare Sicherheitsfunktionen ab Werk deaktiviert sind oder auch erst als ergänzende Leistungspakete (z.B. Datenverschlüsselung) zugekauft werden müssen.

- **Sicherheit ist schwer nachprüfbar und beeinflussbar:** Für Anwender besteht meist nur die Möglichkeit, den Sicherheitsversprechen der Hersteller zu glauben und zu hoffen, nicht eines Besseren belehrt zu werden. Kaum ein Unternehmen kann sich umfangreiche Sicherheitstests (z. B. Penetrationstests) leisten. Die Softwarelösungen sind zumeist „closed source“ (und damit nicht einsehbar). Selbst wenn der Quellcode einsehbar wäre gilt, dass nur wenige Personen die Kompetenz haben, hierin (potenzielle) Sicherheitslücken zu identifizieren, ganz zu schweigen von der Möglichkeit, diese dann auch zu schließen. Sicherheit ist also ein Versprechen, dem man (miss-) trauen muss.

- **Sicherheit ist ein Kompetenz- und Ressourcenproblem:** Kompetenz ist das richtige Stichwort, denn Sicherheit muss oft mehrschichtig gewährleistet werden. Vernetzte Systeme erfordern vernetztes Denken, viel Erfahrung, erhebliche IT-Kompetenzen und den nötigen Freiraum, sich auch wirklich mit Sicherheit auseinandersetzen zu können. „Der IT-Admin für den ganzen Betrieb“ hat eher nicht die Möglichkeit, nebenbei auch noch Sicherheitsthemen zu betreuen. Unternehmen müssen verstehen, dass beim Einsatz von IT die Aspekte „es funktioniert“, „es ist sicher“ und „es ist leicht zu handhaben“ fast so etwas wie ein magisches Dreieck bilden, bei dem immer nur zwei Aspekte gleichzeitig realisiert werden können.

- **Sicherheit ist ein Anwenderproblem:** In der Community gab es schon immer einen geflügelten Ausspruch im Sinne von „das Problem sitzt oft vor dem Computer“. Sicherheit ist maßgeblich ein menschlicher Faktor, wobei der Mensch Systeme sowohl sicherer, als auch unsicherer machen kann. Das beste Sicherheitskonzept nutzt nichts, wenn die Mitarbeitenden sich nicht an die Regeln halten. Provokativ kann ergänzt werden: „Selten ist ein Mensch so kreativ, wie wenn er eine Abkürzung finden muss.“ Hierbei ist aber nicht zu vergessen, dass auch Sicherheitskonzepte Hand und Fuß haben müssen. Die häufige Nutzung von Privatrechnern statt Dienstrechnern in Zeiten des Home-Office, weil beispielsweise die Unternehmensrichtlinien die Nutzung einer bestimmten Plattform für Webmeetings nicht zulassen (diese aber von z. B. Geschäftspartner:innen genutzt wird), ist ein bekanntes Beispiel für schlechte Regeln und den schlechten Umgang mit Regeln.

- **Sicherheit ist nicht „spannend“:** 20 Megapixel sind spannend. Ein Dashboard ist spannend. Automatische Reports, Push-Nachrichten und Remote-Zugriff sind spannend. Sicherheit kann man in der Regel nicht sehen (allenfalls in zusätz-

lichem Aufwand, weil beispielsweise ein kompliziertes Passwort erforderlich ist). Das ist eine Frage der Einstellung und der Wertschätzung, die in Zukunft immer wichtiger werden wird. Mit zunehmender Verbreitung von IoT-Geräten werden sogar unternehmerische Existenzen davon abhängig sein, dass Sicherheit vielleicht doch mal „notgedrungen spannend“ wird.

Erkennen Sie sich, Ihre Mitarbeitenden oder einfach auch Diskussionen im Unternehmen teilweise wieder? Es gibt bisher keine Patentlösung, jedes Unternehmen muss seinen eigenen Weg finden, mit Sicherheit umzugehen. Und: Investieren Sie an den richtigen Stellen?

Weil der falsche Umgang mit Sicherheit tiefgreifende Folgen haben kann (einige Beispiele finden Sie folgend verlinkt), ist es vor allem wichtig, Verantwortung zu übernehmen. Diese Verantwortung kann mit einem „ja“ oder einem „nein“ zu Sicherheit beantwortet werden – aber es sollte eine bewusste Entscheidung sein. Alles andere ist in der fortschreitenden Digitalisierung und der zunehmenden Verbreitung von IoT-Lösungen unverantwortlich.

Schwachstellen in Standardkomponenten, 2 Mio. IoT-Geräte betroffen
https://www.security-insider.de/2-millionen-iot-geraete-von-schwachstellen-betroffen-a-830598/

IoT-Thingbots sind jetzt die größte Gefahr für das Internet
https://www.it-daily.net/it-sicherheit/cybercrime/20291-iot-thingbots-jetzt-groesste-gefahr-fuer-das-internet

Handlungsmöglichkeiten

Sicherheit (z. B. der eigenen Produkte und Prozesse) ist ein essenzieller Bestandteil des Unternehmenserfolgs. Wer IoT-Lösungen im Unternehmen einsetzen will, sollte sich folglich intensiv mit IT-Sicherheit auseinandersetzen. Sind IoT-Lösungen nun unattraktiv? Ja und nein. Wer sich bei den vorherigen Seiten selbst dabei erwischt hat, von dem Thema genervt oder über das „Salz in der Suppe“ vielleicht sogar regelrecht wütend zu sein, der sollte den Nutzen und die potenziellen Kosten einer IoT-Lösung nochmal gut hinterfragen. Wer eine gewisse Skepsis gegenüber IT-Sicherheit entwickelt hat und endlich Lösungen will, bringt eine gute Einstellung für die Digitalisierung mit – denn Herausforderungen verschwinden nicht, wenn man nicht über sie redet. Auf der anderen Seite der Herausforderung „IT-Sicherheit im Internet der Dinge“ wartet nämlich die große bunte Welt der Industrie 4.0 mit ihren smarten Geräten, vernetzten Anlagen, Echtzeitdaten, Fernzugriffen, Selbstregulierung und und und... In diese Welt nachhaltig einzutauchen erfordert es aber, **Sicherheit als geldwertes Gut** zu begreifen, das Wert schützt und schafft. Der Schutz ist offensichtlich: Wo Sicherheit herrscht, kann nur schwer Schaden entstehen. Das Schaffen erfordert mitunter etwas Kreativität: Etwa in Form neuer Geschäftsmodelle, neuer Marketingansätze oder schlichtweg durchgehend guter Kundenreferenzen, aus denen weitere Projekte generiert werden können. Wer in Sicherheit investieren will und kann, dem stehen grundsätzlich unterschiedliche **Lösungsansätze** offen, die folgend (ohne Anspruch auf Vollständigkeit) dargestellt sind:

- **Recherche und Austausch:** Bauen Sie eine eigene Wissensbasis zum Thema „Sicherheit im Internet of Things“ auf. Dokumentieren Sie Vorfälle bei anderen Unternehmen und bei sich selbst, sammeln Sie Sicherheitslösungen und Best Practices. Tauschen Sie sich mit anderen Unternehmen und Expert:innen aus, besuchen Sie Fachmessen. Ziehen Sie die für Sie notwendigen Informationen selbst zusammen, um so Wissen und Kompetenz aufzubauen und weniger von Dritten (z. B. externen Expert:innen) abhängig zu sein.

- **Blacklist und Whitelist:** Halten Sie nach, welche Hersteller, Produkte und / oder Systemkomponenten mit positiven und negativen Schlagzeilen von sich reden machen. Schenken Sie Vertrauen, aber prüfen Sie auch regelmäßig, ob dieses Vertrauen gerechtfertigt ist. Bauen Sie langfristig eine eigene Blacklist (zu meidende Hersteller, Produkte oder Komponenten, z. B. bestimmte Kommunikationsprotokolle) und Whitelist (vertrauenswürdige Hersteller, Produkte oder Komponenten) auf, um sicherheitskritische Entscheidungen schnell und anhand lang geprüfter Kriterien treffen zu können. Hierbei ist generell Augenmaß gefragt, denn es gibt noch keine Kriterien, nach denen IoT-Geräte offiziell als „sicher“ eingestuft werden können.

- **Die Kosten für Sicherheit tragen:** Sicherheit kostet und generell betrachtet bekommen Sie an Sicherheit das, was Sie auch dafür bezahlen. Bezahlen Sie den Preis und finden Sie Wege, diesen marktseitig wieder zu refinanzieren. Nutzen oder entwickeln Sie Methoden zur Ermittlung der Wirtschaftlichkeit, die Sicherheit nicht nur als Kostenfaktor berücksichtigen.

- **Testumgebungen nutzen:** Nutzen oder erschaffen Sie selbst Testumgebungen, um neue Produkte einzeln oder im Verbund „auf Herz und Niere“ zu testen. Die Produktion ist der falsche Ort, um neue Produkte erstmalig einzusetzen.

- **Zero Trust:** Seien Sie dennoch sparsam mit Ihrem Vertrauen. „Zero Trust“ – vollständiges Misstrauen – mag übertrieben wirken, insbesondere wenn z. B. nach Ihren Recherchen dem Hersteller vertraut werden kann und auch diverse Tests die Sicherheit bestätigt haben, aber eine Schutzschicht mehr ist besser als eine Schutzschicht weniger.

- **Marktbeobachtung:** Beobachten Sie den Markt. Wie ist die Dynamik? Wie lange halten Anbieter durch? Wer kauft wen und wie verändert das die Produkte (Anmerkung: anfangs sinkt oft die Qualität)? Welche Interessen stehen hinter den Anbietern und welche Visionen? Wie entwickeln sich Gesetze und Regularien, was ist am Entstehen? Lassen Sie die Erkenntnisse in Ihre Black- und Whitelist einfließen. Merken Sie sich aussichtreiche Kandidaten vor, um diese bei der nächsten guten Gelegenheit auf die Probe zu stellen.

- **IT-Sicherheitskompetenzen ausbauen:** Finden oder bilden Sie eigene Fachkräfte aus. Niemand kennt das Netzwerk besser als derjenige, der es aufgebaut hat und administriert. Machen Sie sich unabhängig von IT-Dienstleistern am Markt, wenn möglich, und bieten Sie darauf aufbauend vielleicht sogar neue Services an. Investieren Sie auch in ein Grundniveau an IT-Sicherheitsverständnis bei ALLEN Mitarbeitenden.

- **Nutzen Sie neue und Best-Practice-Sicherheitsmaßnahmen:** Lernen Sie von den Erfolgreichen. Implementieren Sie Maßnahmen wie die Überwachung des Netzverkehrs auf Anomalien oder die Kombination von Mensch und KI, das Human-Machine-Teaming. Gehen Sie genauso mit der Zeit, wie die Angreifer:innen es tun.

- **Betreiben Sie Risikomanagement:** Analysieren Sie, welche Risiken sich aus IT-Sicherheitsproblemen ergeben können. Ergreifen Sie passende präventive und reaktive Maßnahmen, um Vorfälle zu verhindern oder, wenn das nicht möglich ist, deren Auswirkungen zu minimieren. Passen Sie Ihr Risikomanagement immer wieder neuen Entwicklungen an.

- **Nutzen Sie die Angebote Dritter:** Wenn Sie eigene Maßnahmen nicht umsetzen können oder wollen, dann ist die Einbindung vertrauenswürdiger Dritter eine gute Wahl. Von der Versicherung von Risiken bis zum kompletten IT-Outsourcing kann es unterschiedliche Optionen geben, die für Sie generell oder übergangsweise die optimale Lösung sind. Hüten Sie sich aber dennoch davor zu viel aus der eigenen Hand zu geben, sonst sind Sie im Zweifel zu sehr von der Leistungsfähigkeit Außenstehender abhängig und selbst vielleicht nicht mehr handlungsfähig.

Natürlich ist die Umsetzung einer oder mehrerer dieser Handlungsempfehlungen mit Aufwand verbunden, den sich das Unternehmen auch leisten können muss. Auch wird nicht jedes Unternehmen jeden Lösungsansatz selbst umsetzen können, sondern mitunter auf externe Hilfe angewiesen sein. Hierbei gilt: Machen Sie so viel wie möglich. Wenig ist in diesem Fall nicht mehr, sondern eben wenig. Bauen Sie eigenes Know-how auf oder finden Sie Personen (oder Dienste) mit viel Know-how, denen Sie vertrauen können.
Schwache IT-Sicherheit ist günstig, schnell und vielleicht (zunächst) ausreichend. Doch IT-Sicherheit muss immer mit den Anforderungen und mit der Zeit gehen. Und sie muss gelebt werden. Nur so lassen sich Attacken abwehren. Dies gilt natürlich nicht nur, wenn gänzlich neue Geräte angeschafft werden, sondern auch dann, wenn „alten“ Geräten ein „zweites digitales Leben“ eingehaucht wird – etwa durch Retrofitting. Nun soll es darum gehen, wie die Thematik von IoT und Sicherheit bei der Einbindung von Geräten aussieht, die bisher noch gar kein IT kannten?

Nur 6 % der deutschen Unternehmen sehen sich in IoT-Sicherheit gut aufgestellt
https://www.funkschau.de/sicherheit-datenschutz/94-prozent-der-deutschen-unternehmen-sehen-handlungsbedarf.179530.html

Kurzer Abriss zu Human-Machine-Teaming
https://www.it-daily.net/it-sicherheit/cloud-security/20693-mensch-maschine-teaming-gegen-cyberbedrohungen

Kurzer Abriss zu Zero Trust
https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/

Retrofitting

Durch den von Computer- und Digitaltechnik geprägten Fortschritt verändern und erhöhen sich die Anforderungen an Maschinen und Anlagen. Maschinenen müssen heute jeden einzelnen Prozessschritt überwachen, dokumentieren und frühzeitig auf Fehler oder anstehende Instandhaltungsarbeiten hinweisen. Gerade kleine und mittlere Unternehmen stehen vor der Herausforderung, Anlagen und Maschinen weitestgehend zu digitalisieren, nicht aber funktionierende Bestandsanlagen durch neue ersetzen zu wollen oder zu können.
Dadurch wurde das **„Retrofitting“** zu einem zentralen Konzept der digitalen Transformation: Im traditionellen Sinn bezeichnet Retrofit den Austausch von Teilkomponenten einer Maschine oder Anlage. Das Ziel, die Genauigkeit, die Handhabung, die Geschwindigkeit oder die Wartungsfreundlichkeit wiederherzustellen bzw. zu erhöhen. Das intelligente Retrofitting konzentriert sich darauf, Bestandsmaschinen mit Sensorik und Kommunikationstechnik auszustatten, um relevante Prozessparameter zu erfassen, zu verarbeiten und zu speichern. Daraus ergeben sich verschiedene Chancen und Risiken, die anhand eines Beispiels dargestellt werden sollen.
In diesem Beispiel wird an einer handelsüblichen Standbohrmaschine (siehe Abbildung 1) ein Retrofitting durchgeführt. In der Maschine befindet sich eine integrierte Steuerung, die für die Datenerfassung der Drehzahl sowie der aktuellen Bohrkopfhöhe zuständig ist. Um nicht in den Prozess der Steuerung einzugreifen wird die Maschine um eine weitere Steuerung und ein IoT-Gateway erweitert. Die zusätzliche Steuerung liest die Daten der bereits vorhandenen Steuerung über ein spezifisches

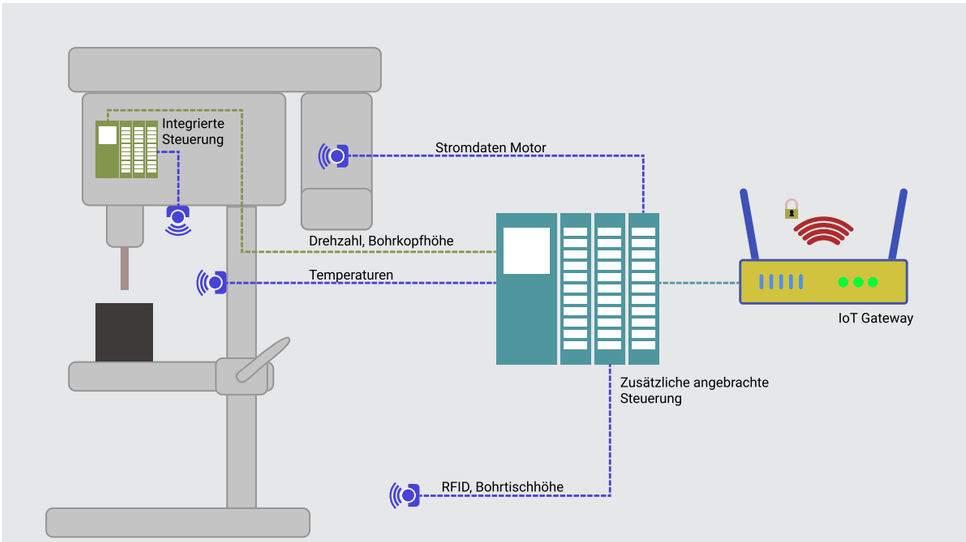


Abbildung 1: Beispielhafte Darstellung von Sensordatenerfassung und -verarbeitung beim Retrofit

Augmented-Reality-Anwendung mit Echtzeitüberwachung

Digitaler Zwilling mit Echtzeitüberwachung

Abbildung 2: Digitalisierung als Grundlage für die Anwendung eines digitalen Zwillings und einer erweiterten Realitätsanwendung (Augmented Reality) für mobile Endgeräte

Protokoll aus. Nachträglich angebrachte Sensoren erfassen weitere Prozessparameter der Maschine. Dadurch können nun zusätzlich die Daten der Motorleistung, der Bohrtischhöhe, der Motortemperatur und der Raumtemperatur überwacht werden. Zudem wurde die Maschine mit zwei RFID-Lesegeräten nachgerüstet. Jeweils ein Lesegerät ist zuständig für die drahtlose Benutzerauthentifizierung und zum Anmelden eines Auftrags an der Maschine. Allein diese eher kleinen Anpassungen bringen verschiedene Vorteile bzw. Chancen mit:

1. **Kosten einsparen.** Erhebliche Kosteneinsparung von Retrofit gegenüber einer Neuanschaffung. Anstatt die Bohrmaschine gegen eine neue Maschine zu ersetzten, verhilft Retrofit der Maschine zu einer verlängerten Lebensdauer.

2. **Potenzial für Verbesserungen.** Die Digitalisierung der einzelnen Prozessparameter schafft eine Grundlage für weitere Optimierungsansätze, z. B. zur Darstellung als digitaler Zwilling, um etwa neue Prozessparameter im Digitalen simulieren zu können, bevor sie im Analogen getestet werden.

3. **Ausfallzeiten reduzieren.** Die Überwachung verschleißanfälliger Bauteile erlaubt es, im Sinne der „vorausschauenden Instandhaltung“ Vorkehrungen zur Wartung schon im Vorfeld zu treffen, bevor das relevante Bauteil ausfällt, um die Stillstandzeiten zu reduzieren.

4. **Qualität steigern.** Durch eine Zugangsbeschränkung nur für autorisierte Benutzer mit speziellen absolvierten Schulungen oder bestimmten Voraussetzungen kann einer fehlerhaften Nutzung vorgebeugt werden. Die Verknüpfung von Benutzern mit Aufträgen erlaubt zudem eine präzisere Steuerung und Auswertung der Produktion.

5. **Kenntnisse der Mitarbeiter behalten ihren Wert.** Ein Austausch von Maschinen ist oft mit neu zu lernenden Handgriffen verbunden. Durch die Weiterverwendung der Maschine kann jahrelang gewonnenes maschinenspezifisches Wissen weiterverwendet werden.

Solche ersten Anpassungen eröffnen zumeist weitere Digitalisierungsprojekte, etwa die Einblendung von Produktionsdaten im Sichtfeld mittels Augmented-Reality-Lösungen oder eben auch die Echtzeitüberwachung der „digitalen Kopie“ der Bohrmaschine, des digitalen Zwillings (siehe Abbildung 2).

Allerdings gibt es dabei auch diverse Risiken:

1. **CE-Konformität/Betriebssicherheit.** Grundsätzlich gibt es drei Vorschriften, die einen Umbau von Maschinen regeln: die Maschinenrichtlinie (MRL 2006/42/EG), die Betriebssicherheitsverordnung (BetrSichV) und das Produktsicherheitsgesetz (ProdSG). Dabei müssen Gefahren und Risiken mitunter neu bewertet werden. Liegt eine wesentliche Änderung vor (Gefahr oder Risiko haben sich geändert) so muss die Maschine wie eine neue behandelt werden und unterliegt somit den Vorschriften zum Inverkehrbringen einer Maschine. Die ausführliche Erklärung zu dieser Thematik können Sie im Retrofit-Leitfaden lesen (s.u.).

2. **Datenschutz.** Werden durch das Retrofitting personenbezogene Daten erfasst, erfordert das laut Datenschutzverordnung (DSGVO) die Einwilligung der betroffenen Personen. Außerdem ist die Zustimmung des Betriebsrates einzuholen, wenn durch Retrofit Verhalten und Leistung der Mitarbeiter:innen überwacht werden können (direkt und indirekt). Weitere Informationen sind dem VDMA-Leitfaden Datenschutz zu entnehmen.

3. **IT-Sicherheitslücken.** Die Digitalisierung von Maschinen und Anlagen und die Erreichbarkeit aus dem Internet birgt den Nachteil, dass sie die Angriffsfläche gegenüber möglichen Cyberattacken erhöht. Das Thema IT-Sicherheit muss in vernetzten Unternehmen einen hohen Stellenwert haben. Was insbesondere auch für das Retrofitting gilt.

Natürlich steht die Standbohrmaschine in diesem Beispiel nur symbolisch für jede andere veraltete Maschine. Je größer und wertvoller die Maschine ist, desto lukrativer ist Retrofitting. Insbesondere Unternehmen, denen (aktuell) die finanziellen Freiheiten für größere Investitionen fehlen, können von Retrofit profitieren. Dabei gilt natürlich auch, dass durch Retrofitting neu vernetzte Geräte auch in Fragen der IT-Sicherheit betrachtet werden müssen.

Zum Retrofit-Leitfaden des VDMA
https://industrie40.vdma.org/documents/4214230/55119136/Leitfaden_I40_Retrofit_Final_1604655010496.pdf

Zum Datenschutz-Leitfaden des VDMA
https://industrie40.vdma.org/documents/4214230/26342484/Leitfaden_Datenschutz_Industrie_40_1529498363948.pdf

Zwischenfazit und Ausblick

In dieser Broschüre kamen die möglichen Chancen des IoT viel zu kurz – hierzu verweisen wir auf die Broschüre **„Internet der Dinge (Internet of Things) – Grundlagen, Anwendungsbereiche, Potenziale“** sowie auf die „Weiterführenden Links“ (s.u.). Insofern ist die Darstellung hier einseitig, denn den hier beschriebenen Risiken stehen auch Chancen gegenüber. Allerdings ist es äußerst wichtig, mit offenen Augen an IoT-Lösungen heranzugehen und die Sicherheitsaspekte eingehend zu beleuchten. Sicherheitspannen, Datendiebstähle und Systemversagen können sich nur wenige Unternehmen (wiederholt) leisten, ohne dadurch dauerhaft Schaden zu nehmen. Die Broschüre zeigt, dass IoT in Unternehmen und privat angekommen ist und immer mehr Anwendung findet. Kein Zufall also, dass die Forschung die Interaktionsmöglichkeiten und -bedingungen zwischen Mensch und Maschine untersucht. Hier einige Kernaussagen aus einer aktuellen Förderbekanntmachung (ähnlich einer Ausschreibung für die Forschung), um neue Sicherheitsverfahren und -werkzeuge für das IoT zu entwickeln:

- Die Vernetzung von Geräten im Internet der Dinge ist wird in den kommenden Jahren weiter zunehmen, Schätzungen zufolge werden im Jahr 2025 bereits mehr als 60 Milliarden IoT-Geräte installiert sein.

- Mittels IoT-Plattformen lassen sich Geräte heutzutage im privaten Smart Home vernetzen und fernsteuern. Intelligente Haustüren, Rollläden und Garagentore erhöhen den Wohnkomfort, erleichtern bei unzureichender Sicherung allerdings auch Einbrechern den Zugang.

- Auch in der Industrie ergeben sich durch den Einsatz von vernetzten Geräten neue Herausforderungen. Fallen sie und damit die Produktion aus, entstehen hohe Kosten. Werden Daten und Betriebsgeheimnisse unbefugt ausgelesen, bedeutet das unter Umständen die Insolvenz.

- Kostendruck in der Entwicklung und Produktion von IoT-Geräten und deren Software wirkt sich auch auf die IT-Sicherheit aus. Oft ist die Rechenleistung und/oder Speicher der Geräte zwar ausreichend für ihren Einsatzzweck, jedoch nicht für Sicherungsmaßnahmen wie automatische Updates oder Virenscanner.

Die Herausforderung kann so formuliert werden: „Mit IoT-Lösungen können die Grenzbereiche der Anwendungsmöglichkeiten und Wirtschaftlichkeit neu definiert werden, es muss aber aufgepasst werden, dass dabei nicht die Kontrolle verloren und über die (Sicherheits-) Klippe gesprungen wird.“
Aus einem ähnlichen Grund wurde für diesen Abschnitt bewusst die Überschrift „Zwischenfazit“ gewählt: IoT-Geräte werden sich noch längere Zeit sehr schnell weiterentwickeln und ebenso das Umfeld, in dem sie eingesetzt werden. In wenigen Worten darf das Zwischenfazit „spannend, aber mit Vorsicht genießen“ lauten – für das Schlussfazit ist es noch viel zu früh.

Richtlinie zur Förderung von Forschungsvorhaben zum Thema „IoT-Sicherheit in Smart Home, Produktion und sensiblen Infrastrukturen“
https://www.bmbf.de/foerderungen/bekanntmachung-3642.html

Weiterführende Links (Auswahl)

- **Artikel: „Die Gefahr durch IoT-Angriffe wird weiter steigen“**
  https://www.security-insider.de/die-gefahr-durch-iot-angriffe-wird-weiter-steigen-a-911902/
- **Artikel: „IoT-Security ist unverzichtbar“**
  https://www.security-insider.de/iot-security-ist-unverzichtbar-a-907966/
- **Artikel: „Optimierte Prozesse vor neuen Geschäftschancen“ – Vorteile und Mehrwerte von IoT-Lösungen**
  https://www.computerwoche.de/a/optimierte-prozesse-vor-neuen-geschaeftschancen,3550509
- **Artikel: „Mehrzahl aller IoT-Systeme ist angreifbar“**
  https://www.security-insider.de/mehrzahl-aller-iot-systeme-ist-angreifbar-a-851231/
- **Artikel: „IoT-Sicherheit – Land in Sicht oder Land unter?“**
  https://www.bigdata-insider.de/iot-sicherheit-land-in-sicht-oder-land-unter-a-1009927/
- **Bericht: „2020 Unit 42 IoT Threat Report“ – Auszug, vollständiger Report unter Angabe der Kontaktdaten ebenfalls verfügbar**
  https://unit42.paloaltonetworks.com/iot-threat-report-2020/; siehe dazu auch den folgenden deutschen **Artikel: „Die Sicherheit für das Internet der Dinge ist mangelhaft“**
  https://www.infopoint-security.de/die-sicherheit-fuer-das-internet-der-dinge-ist-mangelhaft/a23120/
- **Bericht: „Die Lage der IT-Sicherheit in Deutschland 2020“**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2
- **Bericht: „Handlungsfelder im Bereich IoT-Sicherheit“ des nationalen Cyber-Sicherheitsrates**
  https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2020-12-impulspapier-iot.pdf
- **Leitfaden: „IT-Grundschutz“ des BSI**
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- **Leitfaden: „IoT Security Maturity Model: Practitioner’s Guide“ des Industrial Internet Consortium**
  https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2019-02-25.pdf
- **Datenbank / Verzeichnis: „Exploit Database“ – Datenbank von Schwachstellen und Möglichkeiten zu deren Ausnutzung mit fertigen Quellcodes**
  https://www.exploit-db.com
- **Datenbank / Verzeichnis: „MITRE ATT&CK Framework“ – umfangreiche Aufführung beobachteter Angriffsszenarien**
  https://attack.mitre.org

Die Transferstelle IT-Sicherheit im Mittelstand vermittelt Angebote zum Thema IT-Sicherheit und bietet mit dem IT-Sicherheitscheck einen Test der eigenen IT-Sicherheit an. Informationen zu den Projekten unter:
https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Home/home.html

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit. Weitere Informationen finden Sie unter
www.mittelstand-digital.de

Was ist das Mittelstand 4.0-Kompetenzzentrum Cottbus

Das Mittelstand 4.0-Kompetenzzentrum Cottbus setzt sich aus den fünf Partnern BTU Cottbus-Senftenberg (Projektleitung), Technische Hochschule Wildau, Hochschule für nachhaltige Entwicklung Eberswalde, IHP GmbH Leibniz-Institut für innovative Mikroelektronik Frankfurt (Oder) sowie IHK Cottbus als Vertreterin der Landesarbeitsgemeinschaft der Industrie- und Handelskammern in Brandenburg zusammen. Dabei stehen die Schwerpunkte Arbeit 4.0, Digitalisierung in Logistik und Produktion, IT-Sicherheit, Assistenzsysteme, Automatisierungstechnik, Robotik sowie Sozialpartnerschaften im Mittelpunkt. Das Zentrum gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

KONTAKT

Mittelstand 4.0-Kompetenzzentrum Cottbus
c/o Technische Hochschule Wildau
Hochschulring 1
15745 Wildau
Tel.: +49 3375 508782
info@kompetenzzentrum-cottbus.digital
www.kompetenzzentrum-cottbus.digital

Folgen Sie uns: