Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

Jens Dittrich - MDR AdöR
Peter Wickboldt - Universität Rostock

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

- Auf den www-Seiten des BSI erhalten Sie ausreichende Hilfsmittel für eine erste Analyse. -> https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

- Alle nachstehenden Fragen sollten Sie sich stellen, um Schwachpunkte in Ihrem System zu analysieren.

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

- Wer hat in Ihrem Unternehmen Zugang zur Managementebene?
- Wer hat in Ihrem Unternehmen Zugang zur Automationsebene?
- Wer hat in Ihrem Unternehmen Zugang zur Feldebene?
- Nutzen Sie ein Rollen- /Rechtesystem auf der Management- und Automationsebene?
- Wie häufig werden bei Ihnen die Zugangsdaten geändert?
- Welche Systeme nutzen Sie, um Zugriffe auf das System zu überwachen?
- Ist bei Ihnen die Datenschutzbeauftragte / der Datenschutzbeauftragte oder eine IT-Sicherheitsbauftragte / ein Sicherheitsbeauftragter in die Betreibung / Installation der Systeme integriert?

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

- Zugang auf die Feldebene -> LON / KNX
- Zugang auf die Automationsebene -> DDC: passwortgesichert?
- Zugang zu sensiblen Versorgungssystemen -> Wer hat Zugang?
- Wie aktuell ist die Dokumentation?
- Verfügen alle Systeme über die aktuellen Updates?
- Werden für alle Systemkomponenten noch Updates geliefert?
- Wer verwaltet bei Ihnen das Netz und die Systemkomponenten?

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

- Führen Sie regelmäßige Kontrollen der Systeme und der physischen Zugänge durch?
- Gibt es regelmäßige Abstimmung mit den Systemlieferanten zu bestehenden Probleme?
- Verfügt der Bauherr über die erforderliche Kompetenz zur Umsetzung des Mindestmaßes an IT-Sicherheit in der GA?
- Erhalten eine vollständige Dokumentation bei Übergabe der Baumaßnahme inkl. der gesamten Software?
- Setzen Sie BACnet Secure Connect (BACnet/SC) ein?

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

Warum werden GA-Systeme nie wirklich sicher?

- Bequemlichkeit, Gewohnheit
- Personalmangel
- Unwissenheit - fehlende Kompetenz beim Betreiber
- Keine Vorgaben und Kontrollen
- Fehlende wiederkehrende Überprüfung der Systeme
- Eingrenzung der Flexibilität

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

Universität Rostock (Betrieb)

- Kompetenz in der Bauverwaltung (Bauherr) nur beschränkt vorhanden - Diskussions-grundlage fehlt
- Rechte-/Rollensystem umgesetzt, jedoch werden Zugangsdaten nicht regelmäßig geändert
- Gerätelisten, Dokumentation und Updates nicht auf dem aktuellen Stand
- physischer Zugang nur bedingt gesichert
- kryptografisch gesicherte Protokolle (KNX, BACnet SC) noch nicht im Einsatz
- Schnittstellen in IP-Netzwerke nicht vollständig dokumentiert. Verantwortlichkeit / Zuständigkeit unklar

Jens Dittrich - MDR AdöR ; Peter Wickboldt - Universität Rostock

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

Universität Rostock (Betrieb)

- Trennung zwischen GA-Netzwerk (Betrieb durch HKLS-/E-Ing.)
  und IT-Netzwerk (IT-Ing.) muss künftig miteinander „verschmelzen“
- Die erforderliche Einbindung der Datenschutzbeauftragten muss auf beiden Seiten objektiver und funktionaler erfolgen und somit beiden Seiten gerecht werden
- Für die Einbindung des IT-Sicherheitsbeauftragten (ITSO) ist eine umfangreiche Aufklärung von Seiten des laufenden Betriebes und einem realen Risikomanagements erforderlich
- Aktivitäten der Wartungsfirmen müssen künftig besser begleitet werden
- Personalschlüssel muss angepasst werden
- Fehlende Kompetenz muss durch umfangreiche Schulungen und Wissenserweiterung erfolgen

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

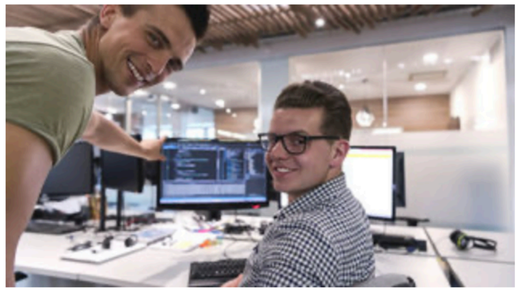
Universität Rostock (Übergaben)

- Kompetenz in der Bauverwaltung (Bauherr) nur beschränkt vorhanden
- In der Ausschreibung wird die GA-Sicherheit nicht fokussiert
- Unzureichende Dokumentation -> Hoffnung auf stärkere Digitalisierung (BIM)
- Unzureichende Einweisung -> im Bereich GA-Sicherheit geringe Information
- Keine ganzheitliche Betrachtung (Zugang, Netzwerkübergänge, TGA-Komponenten)
- Überprüfung der Soft- /Hardware wird nur bedingt umgesetzt
- Bauherr muss sich zu stark auf die Kompetenz des Planers verlassen

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

Das BSI Themen IT-Sicherheitsvorfall Karriere Service

Ich suche grundsätzliche Informationen, um mich vor einem IT-Sicherheitsvorfall zu schützen



Um sich als Unternehmen grundlegend vor einem IT-Sicherheitsvorfall zu schützen, empfiehlt das BSI eine strukturierte und organisierte Herangehensweise. Dazu bietet sich ein Informationssicherheitsmanagementsystem (ISMS) an. Mit dem **› IT-Grundschutz** bietet das BSI eine bewährte Vorgehensweise zur erfolgreichen Umsetzung eines ISMS. Mit unterschiedlichen **› IT-Grundschutzprofilen** und einem **› Routenplaner** haben wir zudem die notwendigen Schritte an Unternehmen unterschiedlicher Branchen und unterschiedlicher Größen angepasst und die Einstiegshürden gesenkt.

Als **› Teilnehmer der Allianz für Cyber-Sicherheit** haben Sie außerdem Zugriff auf zahlreiche Informationspapiere, die durch das BSI oder andere Teilnehmer der Allianz bereitgestellt werden.

Informationen zu ausgesuchten Themen wie dem Schutz vor DDoS, Emotet, Advanced Persistant Threats (APT) uvm., sowie nützliche Tipps finden Sie z. B. auf den **› Themenseiten** des BSI. Empfehlen möchten wir Ihnen u.a. die

Basismaßnahmen der Cyber-Sicherheit v2.0 oder

Management von Schwachstellen und Sicherheitsupdates - Empfehlungen für kleine Unternehmen und Selbstständige v2.0

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

- ☐ Der Bedrohungsgrad der eigenen Infrastruktur sowie die Transparenz der Institution gegenüber Angreifern wurde bestimmt. Daraus wurde die *Cyber-Sicherheits-Exposition* abgeleitet.
- ☐ Sämtliche Netzübergänge sind identifiziert und hinreichend abgesichert.
- ☐ Die Infektion mit Schadprogrammen wird mit wirksamen Maßnahmen unterbunden.
- ☐ Die IT-Systeme wurden inventarisiert und auf ihre sicherheitstechnische Beherrschbarkeit hin geprüft.
- ☐ Offene Sicherheitslücken auf IT-Systeme werden vermieden.
- ☐ Eine Interaktion mit dem Internet findet nur über abgesicherte Komponenten statt.
- ☐ Logdaten werden zentral erfasst und ausgewertet.
- ☐ Die eigene Organisation wird mit allen notwendigen Informationen versorgt.
- ☐ Die Organisation ist auf die Bewältigung von Sicherheitsvorfällen vorbereitet.
- ☐ Die eingesetzten Mechanismen zur Authentisierung verhindern eine missbräuchliche Nutzung durch Dritte.
- ☐ Es stehen ausreichende interne Ressourcen zur Verfügung, externe Dienstleister werden eingebunden.
- ☐ Das eigene Personal wird in Fragen der Cyber-Sicherheit qualifiziert und sensibilisiert.
- ☐ Es werden nutzerorientierte Maßnahmen zur Rollentrennung durchgesetzt.
- ☐ Die Organisation und ihre Mitglieder bewegen sich sicher in Sozialen Netzen.
- ☐ Bei höherem Schutzbedarf werden Vertraulichkeit, Verfügbarkeit und Integrität durch wirksame Maßnahmen gewährleistet und Penetrationstests durchgeführt.
- ☐ Zur Abwehr gezielter Angriffe werden unterstützende Schutzmaßnahmen ergriffen.

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

MDR

Betrieb

- Kompetenz in der Planung und Betreibung begrenzt vorhanden – Schwerpunkt liegt insbesondre im Betrieb auf einer techn. „Sicheren Versorgung“ und überlagert den Blick auf Bedrohungsscenarien und deren Konsequenzen
- BACnet SC noch nicht im Einsatz, KNX SC teilweise (im Aufbau)
- Rechte-/Rollensystem umgesetzt, Standardsystemlösungen werden durch „Standard-IT“ betrieben (z.B. Datenbanklösungen, Backup- & Recovery-Lösungen, Fileservice)
- Dokumentation erfolgt softwaregestützt incl. Inventarisierung und Softwareanalyse,
  Updates werden nach Systemtests ausgerollt – daher hier eine regelmäßige Latenz zum aktuellen Stand
- physischer Zugang zur GT über elektronisches Zugangssystem gesichert, Fehlerquelle Mensch größtes Risiko
- Wartungsfirmen arbeiten oft eigenständig - unbegleitet
- Personalmangel, teilweise fehlende Kompetenz
- Trennung zwischen GA-"Netzwerk" (Betrieb durch Betreiber GA) und IT-Netzwerk (IT)

Das IT-Sicherheitsgesetz: Erfahrungen eines Anwenders

MDR

Herausforderungen

- IT setzt zunehmend neue Schutzsoftware ein - ohne dies mit Nutzern (z.B. GA) abzustimmen. Diese Software arbeitet für den Nutzer oft intransparent - Fehlersuchen werden dadurch deutlich aufwändiger, dauern länger und Personenkreis/Kompetenz der notwendigen Mitwirkenden oft unklar
- Parameteränderungen werden mit bestem Vorsatz (IT-Sicherheit) vorgenommen - Auswirkungen auf die Gebäudetechnik jedoch oft unbekannt (z.B. Blockieren/Abschotten des GT-Netzes zum Internet).
- Großteil der GA basiert auf MS Windows und basiert auf einem Hauptangriffsziel (Plattform) von Schadsoftware und Angriffen.
- unzureichender Support seitens Microsoft für „Nicht-Standard-Umgebungen“.
- Softwareentwicklung der GA-Hersteller berücksichtigt eine geschlossene Umgebung i.d.R. nicht und geht auf ein "normales System". Herstellerseitige Konfigurationshinweise oft zu allgemein und zu unspezifisch.
- Zunehmender Einsatz von „IoT-Endgeräten“ – beliebte Ziele für Hacker (z.B. Ausgangspunkt für DDoS-Angriffe)
- Hoher Spezialisierungsgrad in der IT – Probleme die durch systemübergreifende Zusammenhänge entstehen, sind schwer zu bearbeiten/lösen – IT-Generalist erforderlich.

Wie machen wir weiter ?

- **Wir denken über das Thema nach**
- **Wir prüfen unsere Ressourcen zur Umsetzung der neuen Anforderungen**
- **….**
- **Wir fassen eine Resolution**
- **….**
- **Oder….**

Jens Dittrich - MDR AdöR ; Peter Wickboldt - Universität Rostock

Zusammenarbeitsmodell: IT Sicherheit in der Gebäudetechnik

Zusammenarbeit IT/GA in unserem Gremium

- Regelmäßiger Wissensaustausch (z.B. Unterjährige Videokonferenz(en) zum Thema IT Sicherheit in der Gebäudetechnik)
- Erstellen einer Kontaktliste für Austausch und KnowHow-Transfer
- Gemeinsames Einbinden interner Resoourcen (z.B. eigene IT) und externer Ressourcen (ggf. Firmen mit besonderem Wissen)
- Erarbeiten und Hinterlegen von Lösungsvorschlägen im Sinne „Best-Practice“
  - Know-How-Plattform schaffen (bei Partner oder „GLT-Anwendertagung.de“)
- Zusammenarbeit mit weiteren Gremien (z.B. BIG-EU-FM)
- …