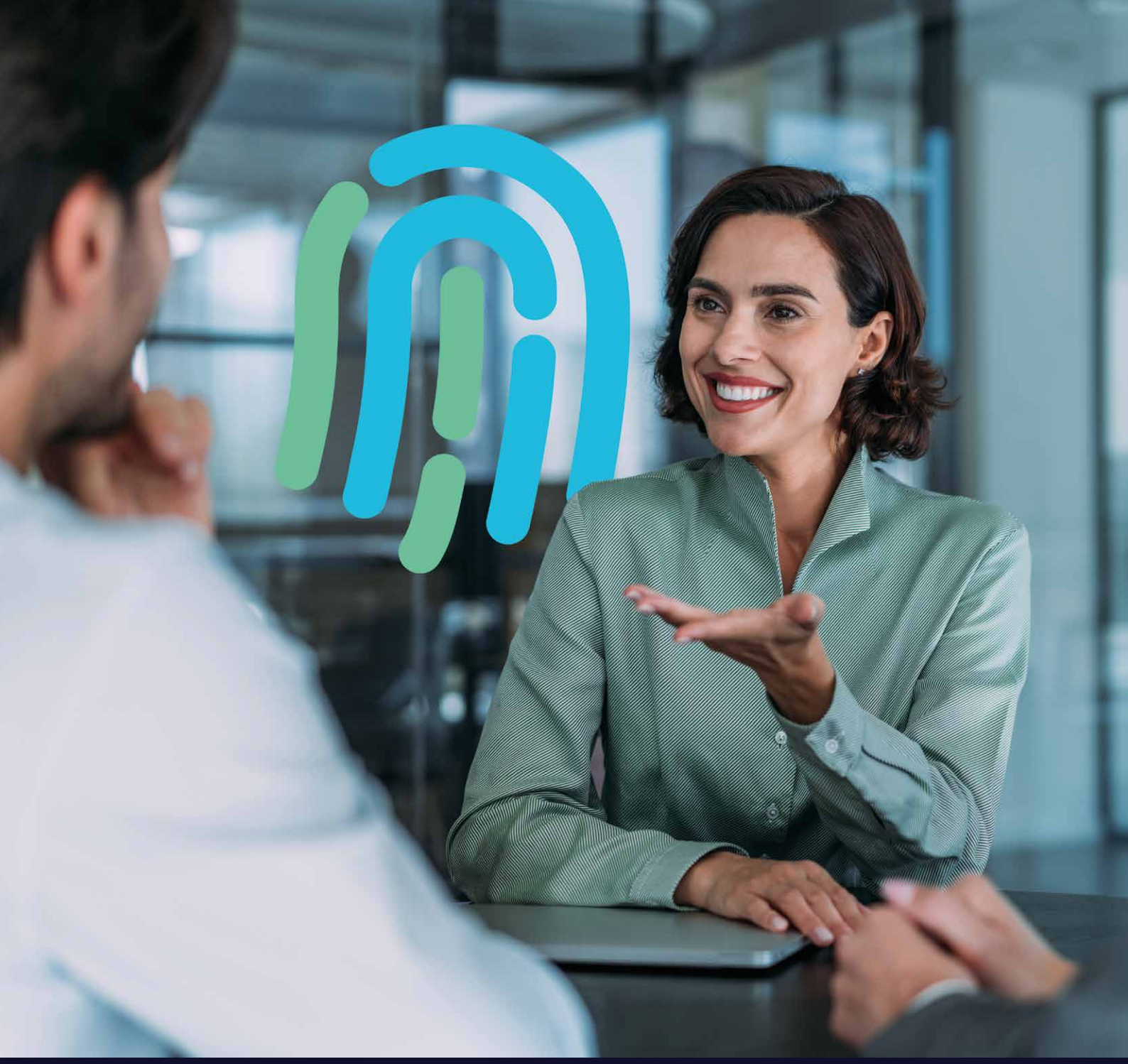


GAP ASSESSMENT IN DER GEBÄUDETECHNIK

Systematische Identifizierung angesichts neuer Herausforderungen

SIEMENS

Der Trend zur Digitalisierung in der Gebäudetechnik und zum „Smart Building“ ist unumkehrbar.

Durch die fortschreitende Digitalisierung der Gebäude- und Sicherheitstechnik werden Gebäude immer vernetzter und intelligenter. Dies bringt neben Komfort, Sicherheit und Effizienz allerdings auch ein erhöhtes Risiko für Cyberattacken mit sich, die sich sowohl gegen Information Technology (IT) als auch Operational Technology (auch Betriebstechnologie, OT) richten. Eine Antwort auf diese spezifischen Herausforderungen in der Gebäudetechnik kann beispielsweise ein Gap Assessment sein, um systematisch potenzielle Sicherheitslücken zu identifizieren. Die gesetzlich vorgeschriebenen Nachhaltigkeitsziele können nur durch eine intelligente Vernetzung der Energiezähler, eine kontinuierliche Datenanalyse und ein effektives Monitoring der Energieverbräuche der Gebäudetechnik erreicht werden. Allerdings birgt die Digitalisierung auch Risiken. So sind Cyberbedrohungen auch in der Gebäudetechnik zu einem allgegenwärtigen Thema geworden. Angesichts dieser Herausforderung ist ein spezifisches Sicherheitskonzept zum Schutz vernetzter Gebäudetechnik unerlässlich.

Kritische Infrastruktur besonders gefährdet

Die Betreiber kritischer Infrastruktur sind von dieser Entwicklung insofern besonders betroffen, als erfolgreiche Cyberattacken nicht nur das Unternehmen, sondern potenziell auch eine große Anzahl an Menschen direkt betreffen. Dazu zählen sowohl Versorgungsunternehmen (wie Energie- und Wasserversorger) als auch Verkehrsbetriebe, Krankenhäuser oder produzierende Unternehmen. Jeder kann sich vorstellen, was es bedeutet, wenn in einem Industriebetrieb die Mitarbeitenden keinen Zugang zum Gebäude oder Gelände haben, wenn die Kühlkette in der Lebensmittel- oder Pharmaindustrie unterbrochen wird oder wenn in einem Operationssaal das Licht ausgeht und nicht mehr eingeschaltet werden kann.

Europäische NIS2-Richtlinie

Für Kritische Infrastrukturen (Kritis) ist das Thema Cyber- und Informationssicherheit naturgemäß besonders relevant. Die EU reagiert darauf mit der NIS2-Richtlinie (Network and Information Security Directive), die seit Jänner 2023 in Kraft ist. Die Richtline hat auch Konsequenzen für die technische Ausstattung von Gebäuden: Zum einen betreffen die Neuregelungen sämtliche Netzwerke inkl. der Gebäudeautomation. Zum anderen gelten praktisch rund 80 % aller Unternehmen und Institutionen in der EU als kritische Infrastruktur im Sinne der Richtline. Das heißt im Umkehrschluss: In 18 definierten Industrie-Sektoren müssen künftig alle Unternehmen mit mehr als 50 Mitarbeitenden bzw. mehr als 10 Mio. Euro Jahresumsatz höhere Cybersecurity-Mindeststandards erfüllen. Auch kleinere Betriebe können von NIS2 betroffen sein, etwa wenn ein Ausfall dieses Betriebes erhebliche Konsequenzen hätte. Auch wenn die Richtlinie noch nicht in nationales Recht überführt wurde, ist es höchst an der Zeit, mit der Umsetzung der entsprechenden Maßnahmen zu beginnen.

Vernetzung erhöht Risiko

Das Risiko für Cyberattacken steigt proportional zur digitalen Vernetzung der Gebäudetechnik. Aktuelle Zahlen des Bundesamts für Sicherheit in der Informationstechnik (BSI-Deutschland) [1] und des Digitalverbands Bitkom (Deutschland) [2] lassen keinen Zweifel daran, dass Cyberbedrohungen zu einem zentralen Thema geworden sind, mit dem wir uns in allen Lebensbereichen verstärkt auseinandersetzen müssen. Im Jahr 2023 wurden mehr als 27.000 Schwachstellen in Softwareprodukten bekannt. Man kann davon ausgehen, dass nahezu jedes österreichische Unternehmen schon einmal von einem Angriff betroffen war.

Das BSI kommt zum Fazit: „Die Bedrohung im Cyberraum ist so hoch wie nie zuvor.“ Unternehmen sind also mit einer Gefährdungslage konfrontiert, für die angemessene Maßnahmen getroffen werden müssen – auch in der Gebäudetechnik. Leider wird sich dieser Trend noch verstärken. Denn die KI hilft nicht nur für „gute“ Zwecke. Schon heute ist KI in der Lage, Teile eines Cyberangriffs zu automatisieren und die Einstiegshürde für Angreifer deutlich zu senken [3].

Schutzmaßnahmen für IT und OT

Glücklicherweise gibt es angesichts dieser bedrohlichen Szenarien auch eine gute Nachricht: Geeignete Präventivmaßnahmen helfen dabei, das Risiko vor, bzw. die Angriffsfläche für Cyberattacken zu verringern, die Widerstandsfähigkeit gegenüber Angriffen zu erhöhen oder zumindest den möglichen Schaden zu begrenzen. Besonders wichtig ist es dabei, dass Sicherheitssysteme fachgerecht aufgesetzt und fortlaufend gepflegt werden. Andernfalls steigt das Risiko für unentdeckte Sicherheitslücken, was zu massiven Zwischenfällen führen kann. Die ganzheitliche Betrachtung von Cybersicherheit im Smart Building wird vor diesem Hintergrund immer wichtiger, denn die Frage für Unternehmen ist nicht, ob sie zum Ziel eines Cyberangriffs werden, sondern wann.

Zu den Quellen gelangen Sie über nachfolgende Kurzlinks:
[1] https://t1p.de/tab12_24_Cyber_BSI; [2] https://t1p.de/tab12_24_Cyber_Bitkom
[3] https://t1p.de/tab12_24_Cyber_BSI2

Gap Assessment und Gebäudetechnik

Ein Gap Assessment bietet eine ganzheitliche Betrachtung des Cybersicherheitsstatus eines Gebäudes. Die Kunden profitieren von einer strukturiert analytischen Vorgehensweise zur effektiven Risikominimierung in Bezug auf mögliche Cyberangriffe.

Das systematische Erkennen und Beseitigen von Sicherheitslücken kann hierbei wie folgt in drei Phasen ablaufen:

1. Discovery Session

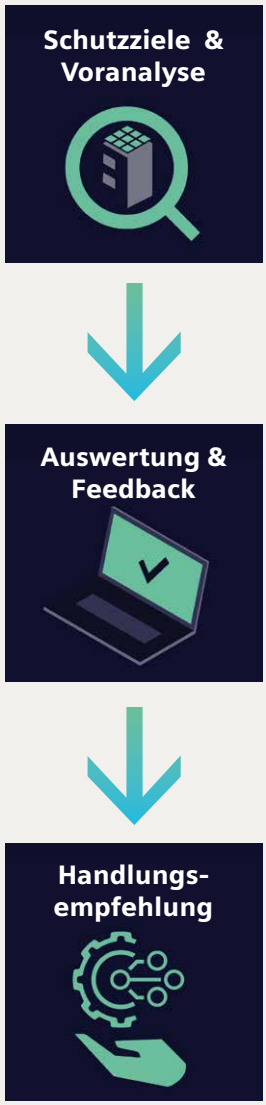
Im Zuge der sogenannten Discovery Session werden die Schutzziele des Unternehmens erörtert. Diese Schutzziele werden oftmals bestimmt durch ein nach ISO 27001 zertifiziertes Informationssicherheits-Managementsystem, durch die Vorgaben der internationalen Normenreihe IEC 62443 („Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“) oder durch branchenspezifische Sicherheitsstandards. Darüber hinaus werden Informationen über kritische Bereiche der Liegenschaft eingeholt und Teilnehmer benannt, die in das Sicherheitskonzept eingebunden sind. Das können etwa Verantwortliche für Gebäudetechnik und die IT-Leitung sein. Anhand dieser Informationen erfolgt eine Voranalyse durch Cybersecurity-Expert:innen sowie die Vorbereitung des nachfolgenden Assessments.

2. Gap Assessment

Das eigentliche Gap Assessment erfolgt im Rahmen eines Workshops inklusive Begehung, der bei Siemens (abhängig von der Größe der Liegenschaften) in der Regel zwei Tage dauert. Am ersten Tag werden beispielsweise Serverstandorte oder Technikzentralen in Augenschein genommen. Darauf folgt ein interviewgestütztes Analyseverfahren. Dabei steht nicht nur die Technik im Fokus, sondern auch Prozesse und Organisation. Am Ende des zweiten Tages erfolgen eine Auswertung und Feedbackrunde mit dem Kunden sowie gegebenenfalls die Vereinbarung eines Folgetermins.

3. Handlungsempfehlung

Der Kunde erhält einen detaillierten Bericht mit Beschreibung der Ist-Situation und einer entsprechenden Handlungsempfehlung. Die Informationen werden als Präsentation aufbereitet, die im Unternehmen verteilt werden kann. Diese Informationen bilden die Basis für den gezielten Einsatz effektiver Sicherheitsmaßnahmen im Unternehmen.



EIN FAZIT

Das Gap Assessment ist der ideale Einstieg in die Cybersicherheit in der Gebäudetechnik und unterstützt insbesondere Kunden, die sich erstmals mit dem Thema auseinandersetzen müssen. Um sich vor Cyber-Angriffen zu schützen, wird es für Unternehmen immer wichtiger, den Status der Cyber-Sicherheit ganzheitlich und systematisch zu erfassen, nicht nur für die IT. Dazu gehört auch die vernetzte digitale Gebäudetechnik/OT.

Mit den aus dem Gap Assessment abgeleiteten Handlungsempfehlungen können die nächsten Schritte zur Umsetzung eines systematischen Cyber-Schutzes für die Gebäudetechnik definiert werden. Die Analyse hilft auch bei der Erfüllung der Cybersecurity-relevanten Gesetze (NIS2 Umsetzungsgesetz). Immer mit dem Ziel vor Augen, das eigene Unternehmen und sein Kerngeschäft besser vor bestehenden Cyber-Risiken auch in der Gebäudetechnik zu schützen.

Kontaktieren Sie uns hier:

siemens.at/cybersecurity-buildings
cys.gebaeude.at@siemens.com