

CyberSafe! Ihr Wissensboost zu Altsysteme

Altsysteme sind in vielen Unternehmen Realität – sei es aus Kostengründen, wegen spezieller Fachanwendungen oder aufgrund fehlender Migrationsoptionen. Genau hier liegt jedoch ein erhebliches Cyber-Risiko: Veraltete Systeme lassen sich oft nicht mehr absichern und werden gezielt von Angreifern ausgenutzt. Jetzt handeln, Risiken durch Altsysteme minimieren und die IT-Infrastruktur zukunftsicher aufstellen!

Trainingsvideo: Altsysteme

Gemeinsam mit unserem IT-Krisendienstleister geben wir praxisnahe Einblicke, wie Risiken durch Altsysteme minimiert werden können. Erhalten Sie im Expertenvideo konkrete Tipps, wie Sie mit gezielten Maßnahmen Ihre IT-Sicherheit optimieren können.

Expertentipps zum Nachlesen

Lesen Sie hier die wichtigsten Take-Aways aus dem Expertenvideo:

- **Altsysteme identifizieren:** Verschaffen Sie sich einen vollständigen Überblick über alle eingesetzten Hard- und Softwaresysteme. Nur wer weiß, was im Einsatz ist, kann Risiken gezielt adressieren.
- **End-of-Life-Fristen beachten:** Prüfen Sie regelmäßig, wann Hersteller den Support für Betriebssysteme und Anwendungen einstellen. Planen Sie rechtzeitig den Umstieg, um Sicherheitslücken zu vermeiden.
- **Risiken durch fehlende Updates vermieden:** Nicht mehr unterstützte Systeme erhalten keine Sicherheitsupdates – bekannte Schwachstellen bleiben offen und werden gezielt von Angreifern ausgenutzt.
- **Altsysteme isolieren:** Altsysteme müssen vom restlichen Netzwerk wirksam abgeschottet, aus zentralen Management- bzw. Authentifizierungsstrukturen herausgelöst und nur über klar definierte, kontrollierte Verbindungen erreichbar sein. Neben einer physischen Trennung kann daher auch eine sauber umgesetzte netzwerkbasierende Segmentierung mit restriktiven Firewall-Regeln eine geeignete Form der Isolation darstellen.
- **Sicherheitsmaßnahmen ergänzen:** Setzen Sie auf zusätzliche Schutzmechanismen wie Firewalls, Antivirensoftware und restriktive Zugriffsrechte, um verbleibende Risiken zu reduzieren.
- **Herstellerkontakt suchen:** Prüfen Sie, ob Updates oder Migrationspfade für Spezialgeräte (z. B. in der Produktion oder Medizintechnik) verfügbar sind.
- **Datenübertragung absichern:** Vermeiden Sie digitale Übertragungswege bei isolierten Systemen – setzen Sie auf physische Medien wie USB-Sticks oder CDs, um sensible Daten sicher zu transportieren.
- **Regelmäßige Überprüfung:** Scannen Sie Ihr Netzwerk auf veraltete Systeme und offene Schwachstellen, um Angriffsflächen frühzeitig zu erkennen.



[Zum Expertenvideo](#)

Hier gelangen Sie zur kompletten Videoreihe „CyberSafe! Ihr Wissensboost für mehr IT-Sicherheit“

[Weitere Videos entdecken](#)

Wissensboost: Altsysteme

Veraltete Systeme können Einfallstor für Cyber-Angriffe sein und gefährden die gesamte IT-Sicherheit. Die gute Nachricht: Wer Altsysteme kennt, bewertet und gezielt absichert, kann das Risiko deutlich reduzieren.

Was versteht man unter Altsystem?

Als Altsysteme gelten Hard- oder Software Komponenten sowie Betriebssysteme,

- die vom Hersteller nicht mehr unterstützt werden,
- keine Sicherheitsupdates mehr erhalten,
- oder nur noch mit unverhältnismäßig hohem Aufwand betrieben werden können.

Warum können Altsysteme ein Risiko darstellen?

Das Problem: Altsysteme erhalten keine Sicherheitsupdates mehr, wodurch bekannte Schwachstellen offen bleiben – und genau diese werden von Cyber-Kriminellen systematisch ausgenutzt.

Checkliste: Das sollten Sie prüfen

Ja	Haben Sie eine vollständige Inventarliste aller Systeme?
Ja	Ist bekannt, ob die verwendeten Systeme noch Updates oder Hersteller-Support erhalten?
Ja	Sind End-of-Life-Daten bekannt und dokumentiert?
Ja	Existieren nicht ablösbare Altsysteme?
Ja	Werden besonders kritische Altsysteme isoliert betrieben? Sind diese von Internet getrennt?
Ja	Ist klar, welche Prozesse von den Altsystemen abhängen und welche Risiken bestehen?
Ja	Sind bestehende Schutzmaßnahmen (z. B. Segmentierung, Zugriffsrechte, starke Authentifizierung, Monitoring) ausreichend?
Ja	Gibt es einen realistischen Modernisierungs- oder Ablöseplan?
Ja	Ist der Cyber-Versicherungsschutz auch für Risiken aus Altsystemen geklärt?

Cyber-Versicherung: Allround-Schutz bei digitalen Risiken

Die genannten Tipps helfen dabei, die Cyber-Sicherheit zu stärken. Leider lässt sich aber auch mit umfassenden Schutzmaßnahmen ein Cyber-Angriff nicht vollständig ausschließen. Um im Ernstfall handlungsfähig zu bleiben, sollten Sie das Restrisiko zusätzlich absichern. Zum Beispiel mit einer Cyber-Versicherung von Hiscox. Als Experte für Cyber-Gefahren und Pionier am deutschen Versicherungsmarkt hält Hiscox Selbstständigen und Unternehmen den Rücken frei – vorbeugend, mitten in der Krise, bei der Schadenregulierung und bei der nachgelagerten Sicherheitsanalyse.

Hiscox

Bernhard-Wicki-Straße 3, 80636 München

Für Makler

T +49 89 54 58 01 100

E hiscox.info@hiscox.de

W makler.hiscox.de/cyber

Für Endkunden

T +49 89 54 58 01 700

E myhiscox@hiscox.de

W hiscox.de/cyber

Hiscox in Social Media

