BSI IT-Grundschutz in der Praxis

„Die Maßnahme ist schon fast umgesetzt“, Erfahrungen aus dem Alltag eines Beraters

Daniel Jedecke – Managing Consultant

HISOLUTIONS

Agenda

1 Vorstellung
2 BSI IT-Grundschutz
3 Herausforderungen in größeren Unternehmen
4 M 5.8 Regelmäßiger Sicherheitscheck des Netzes
5 M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
6 Fazit

HISOLUTIONS

Zur Person

Daniel Jedecke, Managing Consultant der HiSolutions AG, ist seit 2001 in der Informationssicherheit tätig und verfügt über langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen. Er berät und begleitet Unternehmen bei der Einführung von Informationssicherheitsmanagement-Systemen.

Weitere Spezialthemen sind Netzwerksicherheit, PCI DSS und Linux.

Herr Jedecke studierte Diplom-Wirtschaftsinformatik (Dipl. Inf.) an der TH Köln sowie Applied IT Security Master of Science an der Ruhr-Universität Bochum.

Herr Jedecke ist Certified Lead Auditor für Managementsysteme nach ISO 27001, Certified Information Systems Auditor und zertifizierter Datenschutzbeauftragter.

HiSolutions ist eine mehrfach ausgezeichnete Sicherheits-beratung mit über 20 Jahren Erfahrung

Gegründet	1994
Berater	>100
Niederlassungen	Berlin, Frankfurt, Köln, Bonn
Beratungsgebiete	▪ Security Management Consulting ▪ Governance, Risk & Compliance
Kernkunden	▪ Wirtschaft und Industrie ▪ Banken und Versicherung ▪ Regierungen und Behörden
Zertifizierung/ Auszeichnung	▪ BSI-Zertifizierungen als Sicherheitsdienstleister und Penetrationstester ▪ Award for Innovation Berlin/Brandenburg ▪ Zweimal „Fast50 Germany„ und „Fast50 Europe"
Forschung/ Lehre	Lehraufträge an acht Universitäten und Hochschulen in Deutschland und Österreich

HISOLUTIONS

HiSolutions verfügt über eine Vielzahl von Referenzen

HISOLUTIONS

Agenda

1 Vorstellung
2 BSI IT-Grundschutz
3 Herausforderungen in größeren Unternehmen
4 M 5.8 Regelmäßiger Sicherheitscheck des Netzes
5 M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
6 Fazit

HISOLUTIONS

BSI-Standards zur Informationssicherheit (IS)

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

BSI Standard 100-3:
Risikoanalyse auf der Basis von IT-Grundschutz

BSI Standard 100-4:
Notfallmanagement

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

- **Bausteinkataloge**
  - Kapitel B1 "Übergreifende Aspekte"
  - Kapitel B2 "Infrastruktur"
  - Kapitel B3 "IT-Systeme"
  - Kapitel B4 "Netze"
  - Kapitel B5 "IT-Anwendungen"
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

HISOLUTIONS

Agenda

1 Vorstellung
2 BSI IT-Grundschutz
3 Herausforderungen in größeren Unternehmen
4 M 5.8 Regelmäßiger Sicherheitscheck des Netzes
5 M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
6 Fazit

HISOLUTIONS

Herausforderungen in Unternehmen (1 von 2)

- IT-Systemlandschaft historisch gewachsen
  - Dokumentation von Systemen und Anwendungen oft unvollständig
  - Verantwortlichkeiten unklar
  - Komplizierte Vernetzung mit anderen Systemen und Anwendungen
- Tagesgeschäft hat Vorrang vor strategischen Projekten
  - Fokus liegt meist auf der normalen Arbeit
  - Zusätzliche Projekte werden oft vernachlässigt

HISOLUTIONS

Herausforderungen in Unternehmen (2 von 2)

- Abgrenzung der Verantwortlichkeit
  - Unterschiedliche Zuständigkeiten pro Softwarekomponente
    - Langwierige Abstimmungen
    - Kostenintensive Umsetzung von Maßnahmen
    - Ergebnisfindung zumeist nach zeitintensiven Diskussionen und Eskalationen
  - BSI IT-Grundschutz zumeist ein von der IT aus geleitetes Nebenprojekt

HISOLUTIONS

Agenda

1 Vorstellung
2 BSI IT-Grundschutz
3 Herausforderungen in größeren Unternehmen
4 M 5.8 Regelmäßiger Sicherheitscheck des Netzes
5 M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
6 Fazit

HISOLUTIONS

M 5.8 Regelmäßiger Sicherheitscheck des Netzes

- Der Netzadministrator sollte regelmäßig, mindestens monatlich, einen Sicherheitscheck des Netzes durchführen. Für praktisch alle Betriebssysteme sind Programme verfügbar oder bereits im Lieferumfang des Betriebssystems oder der Betriebssystem-Distribution enthalten, die entsprechende Funktionen zur Verfügung stellen. […]

Herausforderungen bei der Umsetzung

- Der Netzwerkadministrator hat meistens nicht die nötigen Berechtigungen um alle Prüfungen durchzuführen
- Die Prüfung der eigenen Systeme kann zu Interessenskonflikten führen
- Es kann beim Sicherheitscheck möglicherweise zu Systemausfällen kommen
- Die Ergebnisse sind meist umfangreich und müssen zielgerichtet an die verantwortlichen Stellen weitergeleitet werden

HISOLUTIONS

Mögliche Hilfen bei der Umsetzung

- Sicherheitscheck sollte von einer unabhängigen Stelle im Unternehmen durchgeführt werden.
  - Zumeist unterhalb der CISO angesiedelt
- Stichproben-Prüfungen können helfen die Last von den Systemen zu nehmen
  - **Wichtig**: Es müssen nicht alle Systeme in einem Sicherheitscheck geprüft werden. Mehrere Sicherheitschecks über ein Quartal verteilt sind sinnvoll (sofern alle Systeme geprüft werden)
- Whitebox Prüfungen (mit Anmeldedaten) sind zumeist wirkungsvoller als Blackbox Prüfungen (ohne weitere Informationen)

Agenda

1 Vorstellung
2 BSI IT-Grundschutz
3 Herausforderungen in größeren Unternehmen
4 M 5.8 Regelmäßiger Sicherheitscheck des Netzes
5 M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
6 Fazit

HISOLUTIONS

M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

- Häufig werden Fehler in Produkten bekannt, die dazu führen können, dass die Informationssicherheit des Informationsverbundes […] beeinträchtigt wird. Entsprechende Fehler können Hardware, Firmware, Betriebssysteme und Anwendungen betreffen. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. […]

Herausforderungen bei der Umsetzung

- Oft werden Informationen über kritische Patches und Updates nicht im Unternehmen weiter gegeben
- Freigabe, Test und Ausrollung können sich über Wochen ziehen
- Patches und Updates werden oft nur als „lästige Aufgaben“ gesehen
- Kritische Updates sollten innerhalb einer Woche meist sogar innerhalb von 1-2 Tagen installiert werden
- Verlust der Garantie oder des Servicevertrags bei Installation von Patches und Updates möglich

Mögliche Hilfen bei der Umsetzung

- Durchführen von Risikoanalysen!
  - Zumeist können Patches und Updates auf interne Systeme später eingespielt werden
- Etablierung eines Patch-Teams
  - Verantwortliche aus allen relevanten Abteilungen sollen schnell Entscheidungen Treffen können
- Aufbau einer produktionsnahen Testumgebung
  - Nur so lassen sich Probleme schnell erkennen
- Haben Sie eine Backup-Strategie?

Agenda

1 Vorstellung
2 BSI IT-Grundschutz
3 Herausforderungen in größeren Unternehmen
4 M 5.8 Regelmäßiger Sicherheitscheck des Netzes
5 M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
6 Fazit

HISOLUTIONS

Zusammenfassung

- Die Planung von Maßnahmen sollte mit allen notwendigen Abteilungen durchgeführt werden
- Setzen Sie abteilungsübergreifende Projekt-Teams ein um notwendige Abstimmungen schnell durchführen zu können
- Prüfen Sie mittels Risikoanalysen ob es alternative Wege zur Umsetzung einer Maßnahme gibt

HISOLUTIONS

So erreichen Sie uns

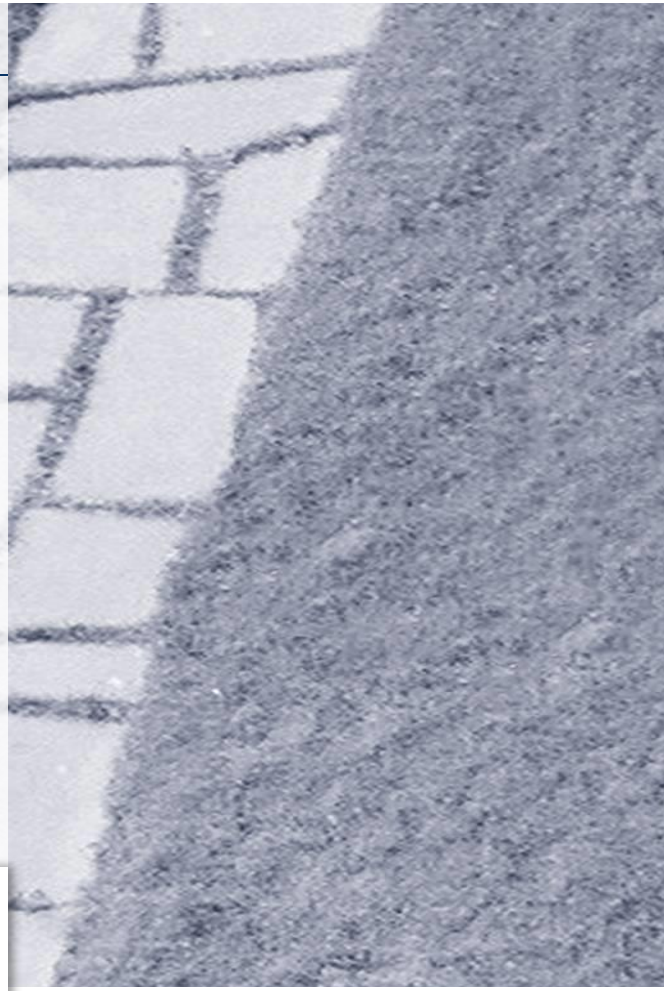
HiSolutions AG

Bouchéstraße 12
12435 Berlin
info@hisolutions.com
www.hisolutions.com
+49 30 533 289 0

Daniel Jedecke

Managing Consultant
Information Security Management
jedecke@hisolutions.com

https://www.xing.com/companies/hisolutionsag
https://www.linkedin.com/company/hisolutions-ag
https://plus.google.com/+HiSolutionsAGBerlin



HISOLUTIONS