Der Weg zum IT-Grundschutz

Erfahrungen aus der erteilten BSI IT-Grundschutz Zertifizierung

Carsten.Gericke@ilink.de

Operative Sicherheit

- Erfahrungen aus dem BSI IT-Grundschutz
  - ISO 27001 auf der Basis von IT-Grundschutz
- Domino, Sametime, Verse
- Keine Theorie - Betriebspraxis

BSI-IGZ-0620

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Zertifikate-ISO-27001-auf-Basis-von-IT-Grundschutz/zertifikate-iso-27001-2024_node.html

Was Sie von dieser Session erwarten können

- Praxisnahe Handlungsempfehlungen
- Erfahrungen aus realen Umgebungen
- Was Sicherheit tatsächlich verbessert
- Kein weiterer Compliance-Vortrag

Zwei Perspektiven auf BSI IT-Grundschutz

1. Der rechtliche / regulatorische Blick

Leitfrage: „Erfüllen wir die regulatorischen Anforderungen?“

BSIG / NIS2 | Compliance | Audits | Nachweispflichten | „Stand der Technik“ | Risikomanagement | Haftung & Governance

2. Der operative/technische Blick auf Sicherheit

Leitfrage: „Können wir Systeme und Informationen zuverlässig schützen und betreiben?“

sicherer Betrieb von IT-Systemen | Schutz von Informationen | Resilienz | Monitoring & Detection | Incident Response | Backup & Recovery | kontinuierliche Verbesserung

Gesetzliche Grundlage

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG)

- § 30 Abs. 1 BSIG
  - „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“
- § 30 Abs. 2 BSIG
  - „Maßnahmen nach Absatz 1 sollen den **Stand der Technik** einhalten …“
- § 30 Abs. 2 BSIG nennt u. a.
  - Risikoanalyse
  - Sicherheitsvorfälle
  - Backup & Wiederherstellung
  - Krisenmanagement
  - Lieferkettensicherheit
  - Schwachstellenmanagement
  - Schulungen
  - Zugriffskontrolle
  - Multi-Faktor-Authentifizierung
- § 31 Abs. 2 BSIG
  - „Dabei soll der **Stand der Technik** eingehalten werden.“

https://www.gesetze-im-internet.de/bsig_2025/index.html

Gesetzliche Grundlage

- Das BSIG beschreibt vor allem:
  - Betrieb
  - Prozesse
  - Überwachung
  - Reaktion auf Vorfälle
  - organisatorische Verantwortung
- Nicht primär einzelne Produktfeatures.

- Kernaussage
  - „Sicherheit entsteht durch Betrieb, Prozesse und Architektur.“

Was erwartet das BSI?

- Angemessene technische und organisatorische Maßnahmen
- Orientierung an Risiko und möglicher Auswirkung
- Sicherheit ist ein Gesamtsystem - kein einzelnes Produkt

Was das BSI-Gesetz tatsächlich sagt

- Maßnahmen müssen dem Stand der Technik entsprechen
- Risikobasierter Ansatz
- Organisatorische und technische Maßnahmen
- Nicht an bestimmte Produkte gebunden

Was sind Sicherheitsmaßnahmen?

- Nicht: ein Produkt kaufen
- Nicht: Standardkonfiguration verwenden
- Sondern: Hardening, Monitoring, Zugriffskontrolle
- Sondern: Segmentierung und Prozesse

- Sicherheitsmaßnahmen sind das, was man tatsächlich tut

Stand der Technik ist kein Produkt

- 😉 Produktdenken
- „Diese Plattform ist sicher“

- 🫶 Operatives Denken
- Architektur, Betrieb, Monitoring

- Sicherheit ist das, was man betreibt

Dasselbe Produkt.
Völlig unterschiedliche Sicherheit

- 😜 Unverwaltetes *«Produkt»*
- Direkte Exponierung, kein Monitoring

- 🫶 Sauber betriebenes *«Produkt»*
- WAF, SIEM, Hardening

- Gleiche Software. Unterschiedliches Sicherheitsniveau

Vom Gesetz zur Umsetzung

- Das Gesetz definiert Erwartungen
- Frameworks definieren Kontrollen
- Der Betrieb setzt Sicherheit um

- Architektur + Prozesse = Sicherheit

Sicherheitsarchitektur

- Logfile-Management
- SIEM-Integration
- Angriffserkennung (IDS)
- Angriffsprävention (IPS)
  - HIDS - Host-Monitoring
  - NIDS - Netzwerk-Monitoring
- Überprüfung der Backup-Integrität
- Penetrationstests
- WAF-Integration
- Security-Proxys / -Gateways

Sicherheitsarchitektur

Unser Zertifizierungszeitplan

BSI-IGZ-0620

Aufbau Infrastruktur

Dokumentation

Internes Review

Initiales Audit

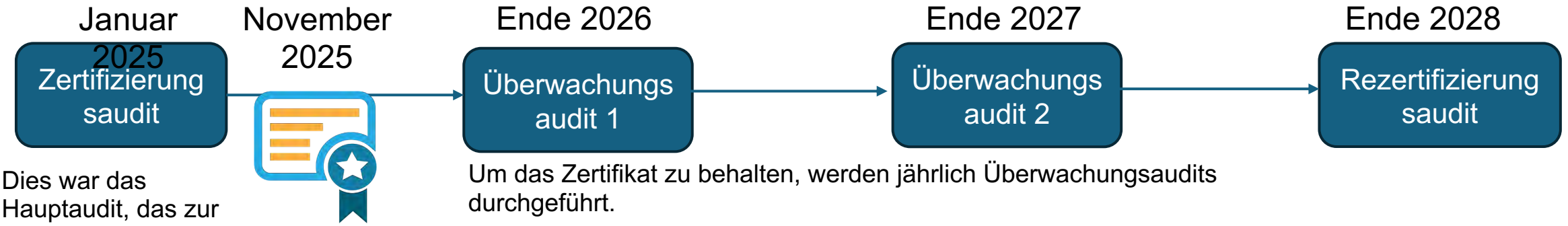
Anpassung

Zertifizierungs-Audit

Bearbeitung des Prüfberichtes durch das BSI

06.05.24	13.05.24	20.05.24	28.06.24	29.07.24	05.08.24	12.08.24	07.01.25	30.01.25	03.03.25	25.11.25
Start Penetration Test	Penetration Test	Vorlage des Berichts	Abschluss Infrastruktur	Dokumenten Einreichung	Initiales Audit	Vorlage des Auditberichts	Dokumenten Einreichung	Vor-Ort Audit		

Betriebszertifizierung für Sametime / Verse / Domino (3-jähriger Audit-Zyklus)



Dies war das Hauptaudit, das zur Ausstellung des Zertifikats führte.

Das BSI hat das Zertifikat ausgestellt.

Um das Zertifikat zu behalten, werden jährlich Überwachungsaudits durchgeführt.

Ihr Zweck besteht darin zu überprüfen, dass:

- das ISMS weiterhin wirksam implementiert und aufrechterhalten wird,
- keine schwerwiegenden Nichtkonformitäten aufgetreten sind, und
- eine kontinuierliche Verbesserung nachgewiesen werden kann.

Interne Audits - Management Reviews - Kontinuierliche Verbesserung

Zusätzlich gibt es fortlaufende interne Aktivitäten innerhalb des ISMS-Zyklus:

- Interne Audits mindestens einmal pro Jahr.
- Management-Bewertungen in regelmäßigen, typischerweise jährlichen Abständen.
- Kontinuierliche Verbesserung und Überwachung von Korrekturmaßnahmen im Rahmen des PDCA-Zyklus.

Sicherheitskontrollen (BSI-Zuordnung)

- Netzwerksicherheit (NET : Netze und Kommunikation)
- Betrieb & Monitoring (OPS: Betrieb)
- Kryptographie (CON: Konzeption und Vorgehensweise)
- Identitäts- & Zugriffsmanagement (ORP: Organisation)
- Business Continuity Management

…

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Grundschutz++

Das BSI entwickelt den Grundschutz weiter

Kontinuierliche Sicherheitssteuerung statt statischer Compliance

Kernidee:

- Sicherheitsanforderungen werden:
  - maschinenlesbar
  - austauschbar
  - automatisierbar
  - kontinuierlich überprüfbar

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Methodik_Grundschutz_PlusPlus.html

OSCAL als Grundlage

Open Security Controls Assessment Language (OSCAL)

Maßnahmen und Nachweise können standardisiert ausgetauscht werden zwischen:

ISMS, SIEM, Audit-Systemen, Vulnerability-Management, Compliance-Tools, Findings & Assessments, etc.

Paradigmenwechsel

- Früher
  - jährliche Audits
  - statische Dokumente
  - manuelle Checklisten
  - punktuelle Bewertungen
- Jetzt
  - kontinuierliche Bewertung
  - automatisierte Reviews
  - laufende Nachweise
  - Operational Security

https://github.com/BSI-Bund/Stand-der-Technik-Bibliothek

BSI.community

Konkrete Maßnahmen für:

- Produkte
- Plattformen
- Betriebsmodelle

werden kollaborativ entwickelt und geteilt.

Grundschutz++ macht Informationssicherheit operational, kontinuierlich und automatisierbar.

https://bsi.community
https://github.com/bsi-community/Stand-der-Technik-Viewer

Stand der Technik ist Ihre Verantwortung

- Sicherheit ist nicht das Produkt
- Sicherheit ist Design, Betrieb und Monitoring

- Stand der Technik ist ein kontinuierlicher Prozess

Top 10 Praktische Sicherheitsmaßnahmen

1. Logging
2. Sicherer Administratorzugang
3. TLS-Hardening
4. Reverse Proxy / WAF
5. Netzwerksegmentierung
6. Backup-Tests
7. Patchmanagement
8. Monitoring
9. Baseline-Konfigurationen
10. Reaktion auf Sicherheitsvorfälle / Incident Response

Nützliche (Open-Source-)Werkzeuge

- ClamAV (Antivirus-Engine zur Erkennung von Trojanern, Viren, Malware und anderen Bedrohungen)
- Snort (Netzwerkbasierte Angriffserkennung (Network Intrusion Detection)
- Falco (Hostbasierte Angriffserkennung / Host Intrusion Detection)
- NGINX + ModSecurity (Web Application Firewall, WAF)
- Borg (Backup- und Archivierungslösung)

Lessons Learned

- 90 % der Probleme sind operativ bedingt
- Dokumentation ≠ Sicherheit
- Werkzeuge benötigen Prozesse
- Auditoren achten auf Nachvollziehbarkeit

Mehrwert

- Schnellere Erkennung von Vorfällen
- Reduzierte Ausfallzeiten
- Klare Verantwortlichkeiten
- Audit-Bereitschaft
- Weniger Chaos

Referenzarchitektur

- *«Produkt»* hinter einem Proxy / Gateway
- Netzwerksegmentierung
- Zentrales Logging
- Dedizierter Administratorzugang
- Optionale WAF / IDS

Stand der Technik

- ❌ Falsch: Ist *«Produkt»* sicher?
- ✅ Richtig: Ist Ihre Implementierung sicher?

- Sicherheit hängt vom Betrieb ab

Wo anfangen?

- Woche 1: Logging
- Woche 2: Administrator-Sicherheit
- Woche 3: Externer Zugriff
- Woche 4: Reaktion auf Sicherheitsvorfälle

Typische Fehler

- TLS = sicher
- Logs werden nicht ausgewertet
- Gemeinsame Administrator-Accounts
- Ungetestete Backups
- Einmalige Sicherheitsprojekte

Das sollten Sie mitnehmen

- Sicherheit ist Betrieb
- IT-Grundschutz liefert Struktur
- Sichtbarkeit, Kontrolle und Disziplin sind entscheidend
- Gehärteter Container nach BSI-Empfehlungen
- Beispiel: ClamAV-Signaturen aktuell halten