NetApp

NETAPP QUICK WINS

Wer NetApp Storage hat ist im Vorteil!

Martin Weilhartner
Principal Account Technology Specialist
März 2024

Quelle: https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

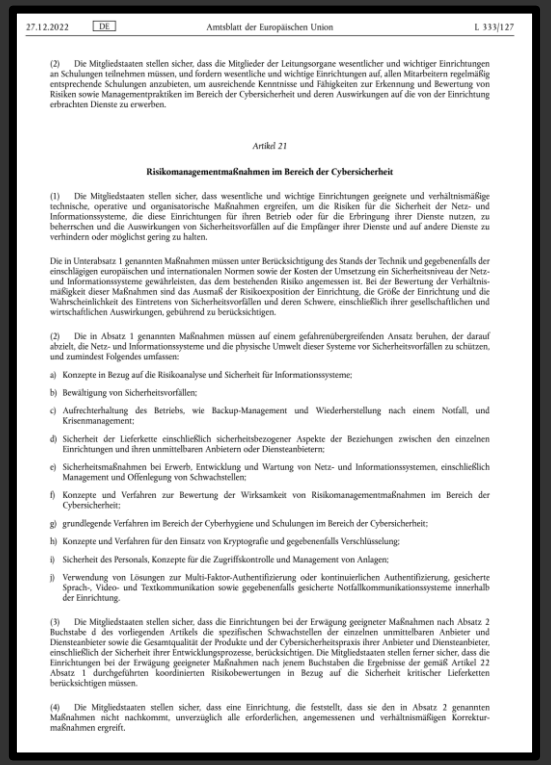
NIS2 Artikel 21

Technische Anforderungen

Konzepte
*zur **Risikoanalyse** und **Sicherheit** der IT-Systeme und zur Bewertung der **Wirksamkeit** der Maßnahmen*

Cyberhygiene und Schulungen

Bewältigung von **Sicherheitsvorfällen**
Erkennung, Analyse, Priorisierung, Vorfallsbehandlung



27.12.2022 DE Amtsblatt der Europäischen Union L 333/127

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleistern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d des vorliegenden Artikels die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Dienstleistungen sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstleistungen, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen. Die Mitgliedstaaten stellen ferner sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach jenem Buchstaben die Ergebnisse der gemäß Artikel 22 Absatz 1 durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten berücksichtigen müssen.

(4) Die Mitgliedstaaten stellen sicher, dass eine Einrichtung, die feststellt, dass sie den in Absatz 2 genannten Maßnahmen nicht nachkommt, unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen ergreift.

Sicherheit des Personals
Zugriffs- / Zutrittskontrollen

Business Continuity
Backup Management, Wiederherstellung im Notfall, Krisenmanagement

Kryptografie und **Verschlüsselung**

Sicherheit der Lieferkette
Beziehungen zwischen Organisationen, Zulieferern und Service Providern

Multi-Faktor Authentifizierung und **gesicherte Kommunikation**
Stimme, Video, Text

Sicherheitsmaßnahmen bei **Erwerb/Entwicklung/Wartung** von IKT
Schwachstellen (Vulnerability) Management und Offenlegung

Business Continuity

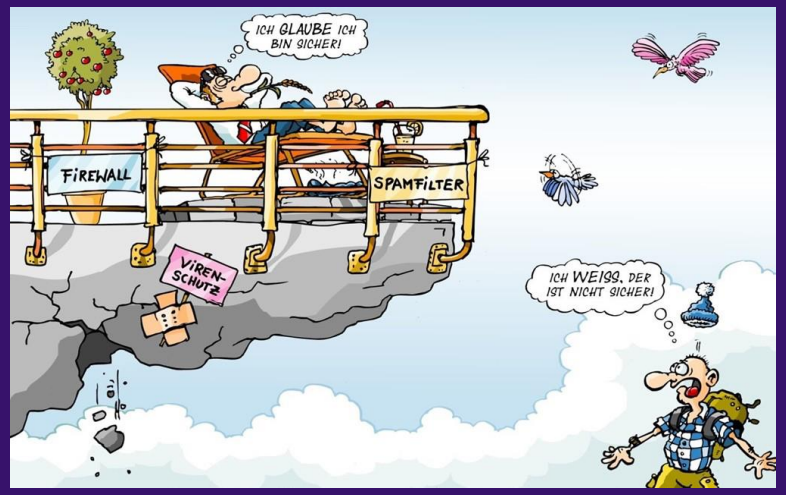
Business Continuity ist entscheidend, um sicherzustellen, dass ein Unternehmen seine Aktivitäten auch in Krisenzeiten weiterhin durchführen kann.

- **Risikobewertung:**
  Identifizierung und Bewertung potenzieller Risiken und Bedrohungen, die die Betriebsabläufe eines Unternehmens stören könnten.
- **Business Impact Analyse (BIA):**
  Klärt Auswirkungen ein Ausfall auf Geschäftsbereiche. Identifiziert die kritischsten Systeme und Prozesse
- **Business Continuity Plans (BCP):**
  Dtaillierte Strategien und Verfahren für den Umgang mit verschiedenen Arten von Störungen.
- **Testen und Überprüfen des Plans**
  Wird gerne ausgelassen!
- **Fortlaufende Überwachung und Aktualisierung:**
  Die Risiken und Bedrohungen für ein Unternehmen ändern sich ständig, ebenso wie die internen Betriebsabläufe.

Typische Angriffe

…aus der Datenmanagement Brille

- Übernahme administrative Accounts
- Löschen oder unbrauchbarmachen von Backups
- Verschlüsseln von Daten
- Daten absaugen
- Typische Dauer eines Angriffes Tagen bis Monate



Ursache für Erfolgreiche Angriffe:

- Falsche Einschätzung der Bedrohung!!!
- Alte Software. Und Firmwarestände
- Lücken die durch Tests entstehen

Source: pwc 2023

Cyber-Risikomanagement

NetApp unterstützt sie mit zahlreichen Lösungen und Dienstleistungen

Datenanalyse: Was liegt wo!

Was sind übliche Angriffe und welche Schutzmaßnahmen gibt es

Datennahe Angriffserkennung

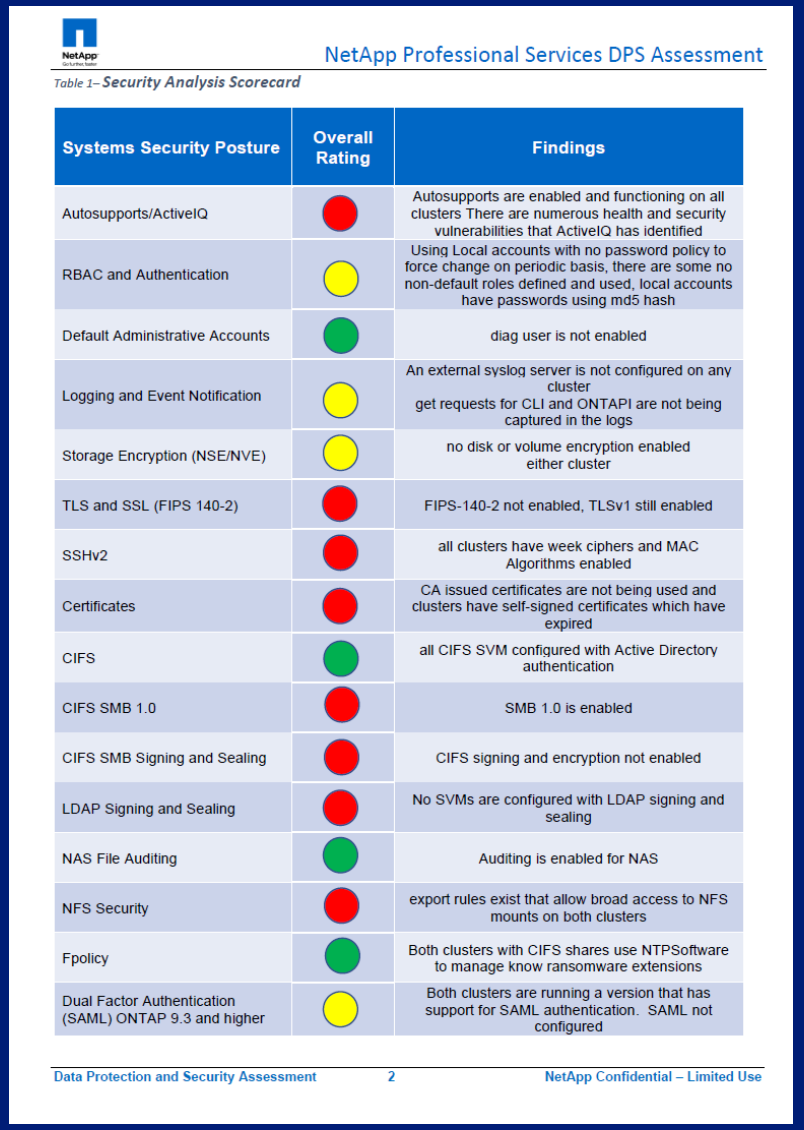
Optimierung beim Schutz und der Wiederherstellung

Analytics & Auditing

Monitoring & kontinuierliche Assessments

Beispiel: NetApp Security Assessment

- Analysis Scorecard
- Empfehlungen für Quick Win’s
- Monitoring & Verbesserung (jährlich, oder öfter)
- Gemeinsames entwickeln einer Strategie



NetApp Professional Services DPS Assessment

Table 1– Security Analysis Scorecard

Systems Security Posture	Overall Rating	Findings
Autosupports/ActiveIQ	🔴	Autosupports are enabled and functioning on all clusters There are numerous health and security vulnerabilities that ActiveIQ has identified
RBAC and Authentication	🟡	Using Local accounts with no password policy to force change on periodic basis, there are some no non-default roles defined and used, local accounts have passwords using md5 hash
Default Administrative Accounts	🟢	diag user is not enabled
Logging and Event Notification	🟡	An external syslog server is not configured on any cluster get requests for CLI and ONTAPI are not being captured in the logs
Storage Encryption (NSE/NVE)	🟡	no disk or volume encryption enabled either cluster
TLS and SSL (FIPS 140-2)	🔴	FIPS-140-2 not enabled, TLSv1 still enabled
SSHv2	🔴	all clusters have week ciphers and MAC Algorithms enabled
Certificates	🔴	CA issued certificates are not being used and clusters have self-signed certificates which have expired
CIFS	🟢	all CIFS SVM configured with Active Directory authentication
CIFS SMB 1.0	🔴	SMB 1.0 is enabled
CIFS SMB Signing and Sealing	🔴	CIFS signing and encryption not enabled
LDAP Signing and Sealing	🔴	No SVMs are configured with LDAP signing and sealing
NAS File Auditing	🟢	Auditing is enabled for NAS
NFS Security	🔴	export rules exist that allow broad access to NFS mounts on both clusters
Fpolicy	🟢	Both clusters with CIFS shares use NTPSoftware to manage know ransomware extensions
Dual Factor Authentication (SAML) ONTAP 9.3 and higher	🟡	Both clusters are running a version that has support for SAML authentication. SAML not configured

Data Protection and Security Assessment 2 NetApp Confidential – Limited Use

Umfassender Schutz gegen Ransomware

ONTAP hat einen umfassenden Schutz gegen Ransomware in das Storagesystem integriert

Snapshots sind unlöschbar und werden mit einem Ablaufdatum versehen

Snapshots lassen sich innerhalb von Sekunden wiederherstellen

Eingebaute Intelligenz erkennt Ransomware und löst einen Snapshot aus

Ein Administrator alleine darf keine destruktiven Operationen durchführen

Verdächtige Benutzeraktivitäten werden blockiert

NetApp Ransomware Recovery Assurance Service

Aktiviert das Ransomware-Recovery-Garantie-Programm

Konfiguration und Reporting

Implementiert und konfiguriert unveränderliche, nicht löschbare Snapshots

- NetApp SnapLock Compliance
- NetApp SnapMirror Vault (auch bekannt als SnapVault)
- Konfigurationsbericht zu SnapLock Compliance Volume

Testen und Wiederherstellen

Beschleunigt die Datenwiederherstellung

- Erstellung eines P1-Vorfalls und Abstimmung des Incident-Managements mit dem Kunden
- Handelt es sich um Fehlalarm oder um einen verifizierten Angriff?
- Rollback von NetApp Snapshot Kopien, sofern notwendig
- Wiederherstellung auf Volume- oder Dateiebene
- Durchführung von Daten-Recovery-Tests

Abonnement-basierter Service

Allgemeine Sicherheitsmaßnahmen

ONTAP Secure by Design

- Verschlüsselung der Daten während des Transports und bei der Ablage
- Gesicherte Netzwerkkommunikation für Administration
- Role-Based Access Control (RBAC)
- Multifaktor Anmeldung für Administratoren; Multi Admin Verifizierung
- Open Authorization (OAuth) Anmeldung für Automatisierung und Anwendungsintegration
- Unterstützung von Netzwerk Sicherheitszonen (IP-Spaces)

DANKE

Wo man uns findet:

Wie man mich kontaktiert:

Jetzt in Kontakt treten

NetApp