SerNet

NIS 2
kurzer Überblick

Dr. Johannes Loxen

SerNet GmbH, Göttingen – Berlin – San Francisco

https://loxen.de/nis2.pdf

SerNet GmbH

SerNet

- gegründet 1997, Büros in Göttingen und Berlin
- Tochterfirma „SerNet, Inc.“ in Kalifornien
- Schwerpunkt Informationssicherheit und Datenschutz
- Produkte und Dienstleistungen rund um Sichere Infrastruktur
  - Firewalls, VPN, E-Mail, Archivierung, Virtualisierung, Hybride Cloud, M365
- verinice.: Open Source ISMS-Tool für Informations-Sicherheits-Management
- SAMBA+: Open Source Alternative zu Windows-Servern, IAM
- SerNet ist klassischer Mittelstand: private Hand, kein Risiko-Kapital, keine Kredite
- über 5000 Bestandskunden in Deutschland, Europa, USA und weltweit

NIS 2

SerNet

- Europäische Verordnung gilt in allen Staaten gleich
  - Beispiel: DSGVO
- Europäische Richtlinie muss in nationales Gesetz umgesetzt werden
  - Beispiel NIS 2
- NIS2UmsuCG kommt hoffentlich rechtzeitig
  - KRITIS-Gesetz, BSI-Gesetz, Energie-Wirtschafts-Gesetz uvm.
- Deadline
  - 18. Oktober 2024

Betroffenheit 1

SerNet

- Mindestens mittleres Unternehmen (50 MA, 10 M€ Umsatz/Bilanz)
- Alle 10 KRITIS Sektoren:
  Energie, Transport und Verkehr, Wasser, Finanz- und Versicherungswesen, Ernährung, Medien und Kultur, Staat und Verwaltung, Gesundheit sowie Informationstechnik und Telekommunikation, dazu IKT & Weltraum
- IKT: DNS-Dienste, Cloud-Computing-Dienste, RZ-Dienste
- Post und Kurierdienste, Abfallwirtschaft, Chemische Industrie, Lebensmittel,
- Siehe NACE Rev.2 Abschnitt C, Abteilungen 26-30
  Hersteller: Medizinprodukte, DV-Geräte, elektrische Ausrüstung, Maschinenbau, KFZ

Betroffenheit 2

SerNet

- Digitale Dienste: Online-Marktplätze, Suchmaschinen, soziale Netze
- Forschung
- „Anbieter verwalteter Dienste“
  (Eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt)
- Anbieter von Domain-Registrierungen und DNS-Anbieter unabhängig von der Größe!

Prüfung der Aufsichtsbehörde

SerNet

- Wenn etwas passiert ist oder man gemeldet wurde, kann das BSI ein ganzes Bündel von Maßnahmen durchsetzen:
- vor-Ort-Kontrollen
- gezielte Sicherheitsüberprüfungen
- Sicherheits-Scans durchführen
- Anforderung von Informationen zur nachträglichen Bewertung
- Zugang zu Daten und Dokumenten
- Anforderung von Nachweisen erfolgter Konzept-Umsetzungen
- KRITIS/wesentlich: ad-hoc-Prüfungen ohne Ankündigung

Technische Maßnahmen

SerNet

- Firewall-Konfiguration
  - Multi-Tier, Mailfilter, VPN, WAF
- Cloud-Konfiguration
  - MFA, Compliance (Datenschutz), Backup
- Endpoint Security
  - PCs, Laptops, Tablets, Smartphones, Wearables, Kassen
- Schwachstellen-Management
  - Scanner, IDS/IPS, Pentests, Updates/Patches
- NAC – Network Access Control
  - Layer 2: Switches & WLAN

Konsequenzen

SerNet

- Meldepflicht bei der Aufsichtsbehörde:
  - in Deutschland beim BSI
  - diese wiederum koordiniert mit ENISA europaweit
- Meldefristen bei Vorfällen
  - schwerwiegender Vorfall innerhalb von 24 Stunden
  - nachfolgend Lagebild innerhalb von 72 Stunden
  - Abschlussbericht nach 1 Monat
- Verpflichtende Schulungen für Geschäftsleitung
- Risiko-Analyse und -Management
- Bußgelder analog zur DSGVO, als Anteil vom Jahresumsatz, max 4%

Kontakt

SerNet

Dr. Johannes Loxen, jl@sernet.de

SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen

tel +49 (551) 370000-0

http://www.sernet.de
kontakt@sernet.de

SerNet, Inc.
101 Montgomery St, #1900
San Francisco CA 94104

+1 (415) 248-7818

http://www.sernet.com
contakt@sernet.com