Acronis

NIS-2
Cyber-Resilienz

Markus Bauer
Senior Technology Evangelist EMEA

Agenda

- **Cyberbedrohungen** aktuell
- **NIS-2** im Überblick
- Anforderungen durch **NIS-2**
- **CSG** in Liechtenstein
- Wie könnte **Acronis** helfen?

Cyberattacken aktuell

Top-3-Bedrohungen je Zielgruppe:

Gesellschaft

Identitätsdiebstahl
Sextortion
Phishing

Wirtschaft

Ransomware
Abhängigkeit innerhalb der IT-Supply-Chain
Schwachstellen, offene oder falsch konfigurierte Onlineserver

Staat und Verwaltung

Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Onlineserver

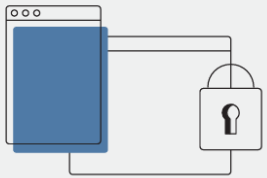
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410

Cyberattacken aktuell

Ransomware

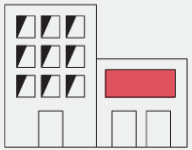
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



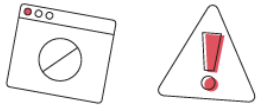
68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister**.

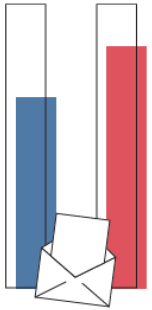


Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion
neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



66%
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84%
aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410

Angriffe auf kritische Infrastruktur in Europa

1. **Viasat-Hack** (24. Februar 2022): Am Tag des russischen Einmarschs in die Ukraine wurde das Satelliteninternet-Netzwerk KA-SAT von Viasat durch einen Cyberangriff gestört. Dies führte zu Ausfällen bei Tausenden von Modems und beeinträchtigte unter anderem die Fernsteuerung von 5.800 Windturbinen in Deutschland.

2. **Cyberangriffe auf deutsche Flughäfen und Behörden** (Frühjahr 2023): Im Frühjahr 2023 wurden deutsche Flughäfen, Landesbehörden und die Polizei Ziel von DDoS-Angriffen, die die Verwundbarkeit kritischer Infrastrukturen deutlich machten.

3. **Cyberangriff auf die CDU** (Juni 2024): Eine Woche vor der Europawahl wurde die CDU Opfer eines schweren Cyberangriffs. Der Verfassungsschutz und das Bundesamt für Sicherheit in der Informationstechnik (BSI) waren intensiv mit den Ermittlungen und Abwehrmaßnahmen beschäftigt.

4. **Cyberangriffe auf Zypern** (Oktober 2024): Zwischen dem 18. und 19. Oktober 2024 wurden mehrere zypriotische Organisationen, darunter Hermes Airports und die Elektrizitätsbehörde von Zypern, Ziel von Cyberangriffen. Die Angriffe wurden von der Hackergruppe LulzSec Black durchgeführt, blieben jedoch weitgehend erfolglos.

5. **Beschädigung von Unterseekabeln in der Ostsee** (18. November 2024): Zwei Unterseekabel, die Litauen mit Schweden und Finnland mit Deutschland verbinden, wurden beschädigt, was zu erheblichen Störungen in der Telekommunikation führte. Deutsche Behörden vermuten Sabotage hinter diesen Vorfällen.

Diese Vorfälle unterstreichen die Notwendigkeit robuster Cybersicherheitsmaßnahmen zum Schutz kritischer Infrastrukturen in Europa.

Cyberkriminalität in Liechtenstein

- In Liechtenstein ist die Cyberkriminalität ein wachsendes Anliegen. Laut einer Studie der Universität Liechtenstein aus dem Jahr 2020 berichtete jedes zweite Unternehmen im Land, bereits Opfer eines Cyberangriffs geworden zu sein.
- Die Kriminalstatistik 2022 zeigt einen minimalen Anstieg der Cyberkriminalität. Allerdings könnten die tatsächlichen Fallzahlen höher sein, da nicht alle Vorfälle gemeldet werden. Die Aufklärungsrate für Cyberkriminalität im engeren Sinne liegt bei 58 %.
- Im Juli 2024 wurden die Websites der Landesverwaltung und der Regierung durch DDoS-Angriffe lahmgelegt. Die genauen Hintergründe dieser Angriffe sind noch nicht bekannt.
- Die Stabsstelle Cyber-Sicherheit fungiert als zentrale Anlaufstelle für den Umgang mit Cyber-Risiken in Liechtenstein.
- Diese Informationen verdeutlichen die Bedeutung von Cybersicherheit für Unternehmen und Institutionen in Liechtenstein.

Acronis

Die Frage ist nicht ob, sondern wann?

#CyberFit

Typische Vektoren für Cyberangriffe

Wie gelangen die Angreifer in die Unternehmen?

Bösartige Nachricht

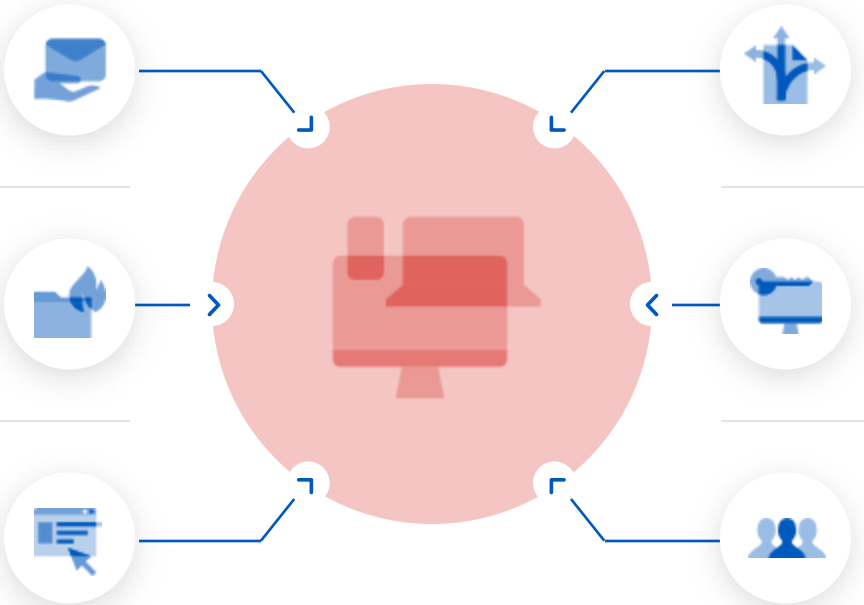
- E-Mail-Anhang
- Social Engineering
- ChatGPT & Co.

Einen Dienst ausnutzen

- Ungepatchter Dienst
- Dateilose Angriffe
- Falsch konfiguriert

Bösartige Cloud/Websites

- Missbrauch des vertrauenswürdigen Standorts
- Handbuch Download
- Umleitung / Site-to-site-Übernahme



Angriff auf die Lieferkette

- Vollständiger Anbieterkompromiss
- SaaS/MSP-Übernahme
- Ansteckung durch Abhängigkeit

Bekannte Berechtigungsnachweise

- Brute-Force-Passwort
- Credential Stuffing / Phishing
- Bezahlter Dropper / Initial Access Broker

Der menschliche Faktor

- Insider-Hilfe
- Menschliches Versagen / Komplexität
- Physischer Zugang

Asymmetrische Angriffe

Angreifer

Minimaler Aufwand

Wenig Fachwissen

Schnell und skalierbar

Verteidiger

Große Anstrengung

Fachwissen erforderlich

Zeitaufwendig

Alter Ansatz | Mauer und Graben


Neue Realität
Lebender Organismus

NIS2 auf einen Blick

Erweiteter Anwendungsbereich

- 18 Sektoren (7 wesentliche, 11 wichtige)
- Schwellenwert: >50 Beschäftigte & >10 Mio. EUR Jahresumsatz

Wichtige Pflichten

- **Leitungsorgane**: Risikomanagement überwachen, Cybersicherheits-Schulungen
- **Meldepflichten**: Frühwarnung (24h), Abschlussbericht (1 Monat)
- **Kontrollen durch Behördern**:
  Regelmäßige Überprüfungen,
  Bußgelder bis zu 10 Mio EUR oder 2% des Umsatzes

Risikomanagement

- Risikoanalyse, Sicherheitskonzepte, Vorfallbewältigung, Krisenmanagement, Lieferkettensicherheit

Weitere Vorgaben

- **Cyber Resilience Act**
- Funkanlagenrichtlinie (RED)

Erhöhte Anforderungen

- NIS2 erhöht die Cyberresilienz im EU-Binnenmarkt
- Erhöhter regulatorischer Druck auf Unternehmen
- Strengere Anforderungen für den Umgang mit Sicherheitsvorfällen
- Höhere Schutzanforderungen durch umfassende Sicherheitsmaßnahmen
- Massive Haftungsrisiken für das Top Management
- Sanktionsrisiken durch Aufsichtsbehörden

Gemeinsame Ziele

Ziel von NIS2

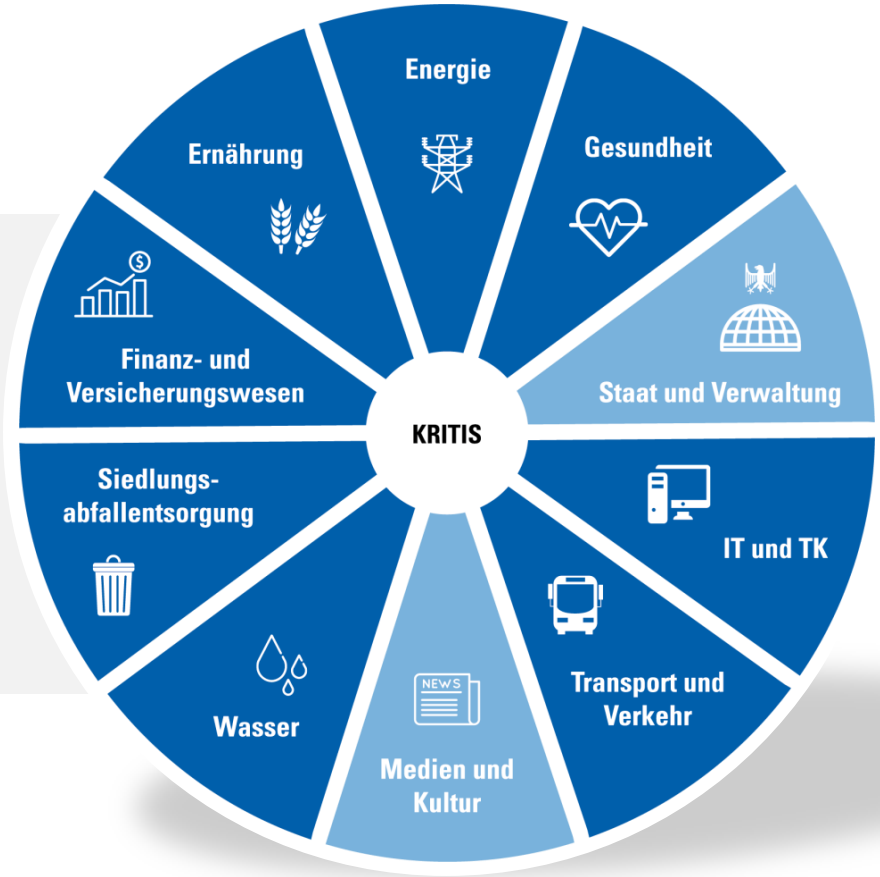
Europa zu einem sichereren Ort zum Leben und Arbeiten zu machen. Den Datenverkehr zwischen Unternehmen und Partnern in Europa und auf der ganzen Welt zu erleichtern.

Ziel von Acronis

Wir schützen die Daten, Applikationen und Systeme sowie die Produktivität eines jeden Unternehmens, indem wir sie vor Cyberangriffen, Hardware-Ausfällen, Naturkatastrophen oder menschlichen Fehlern bewahren, um einen sicheren Arbeitsort zu haben.

Welche Sektoren sind betroffen?

	Beschäftigte (VZÄ)	Jahresumsatz	Jahresbilanz-summe
Kleines Unternehmen (KU)	< 50 und	≤ 10 Mio. Euro oder	≤ 10 Mio. Euro
Mittleres Unternehmen (MU)	< 250 und	≤ 50 Mio. Euro oder	≤ 43 Mio. Euro
Großes Unternehmen (GU)	≥ 250 oder	> 50 Mio. Euro und	> 43 Mio. Euro



Gesetzliche Anforderungen nach NIS2

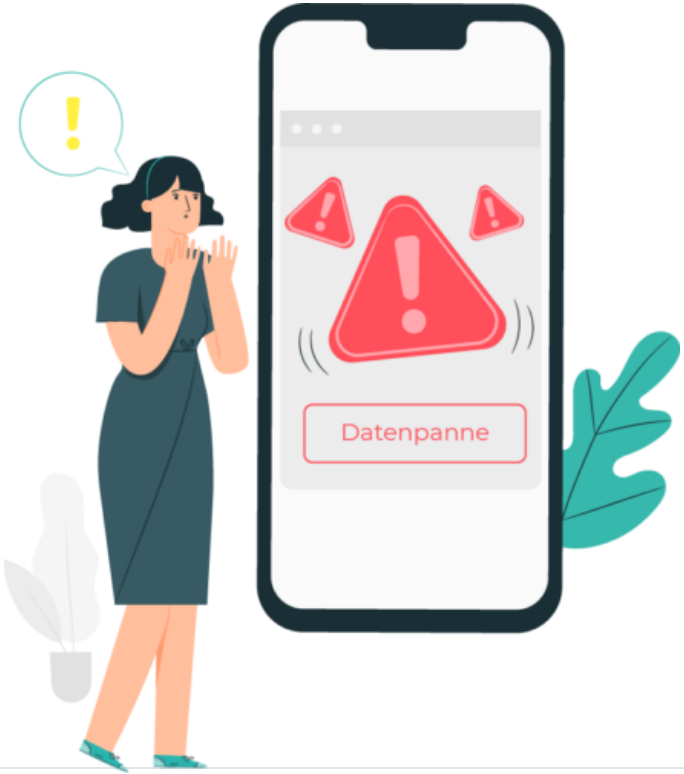
§ 30 Abs. 2 BSIG n. F.

- **Risikomanagement:** Risikoanalyse, Sicherheitskonzepte
- **Sicherheitsvorfälle:** Vorfallbewältigung, Krisenmanagement, Wiederherstellung (Backup-Management)
- **Lieferkettensicherheit:** Sicherheit der Lieferkette, zwischen Einrichtungen, Dienstleister-Sicherheit
- **Systementwicklung:** Sicherheit in Entwicklung, Beschaffung und Wartung
- **Schwachstellenmanagement:** Erkennung und Management
- **Kommunikation:** Sichere Notfallkommunikation, sichere Kommunikation (Sprache, Video, Text)
- **Bewertung:** Effektivitätsbewertung von Cybersicherheit und Risikomanagement
- **Schulungen:** Cybersicherheit und Cyberhygiene
- **Kryptografie:** Einsatz von Verschlüsselung
- **Personalsicherheit:** Zugriffskontrolle, Anlagen-Management, Multi-Faktor-Authentifizierung

Meldepflichten

Im Falle eines Sicherheitsvorfalls ist ein **neuer vierstufiger Meldeprozess** an das BSI zu erwarten:

1. Frühe Erstmeldung binnen 24 Stunden
2. Aktualisierung der Meldung binnen 72 Stunden mit Bewertung der Erstmeldung (Schwere, Auswirkungen und Kompromittierung)
3. Ad-hoc Antworten auf Anfragen des BSI
4. Abschlussmeldung binnen eines Monats



Cyber-Sicherheitsgesetz (CSG)

Überblick und Schlüsselbereiche

Gegenstand und Geltungsbereich

Ziel: Hohes Cybersicherheitsniveau für öffentliche und private Einrichtungen

Anwendbar auf:

- Mittelgroße oder große Unternehmen gemäß Personen- und Gesellschaftsrecht
- Einrichtungen mit besonderer Bedeutung für kritische gesellschaftliche Funktionen (z. B. digitale Infrastruktur, Gesundheitswesen, Energieversorgung)

Schlüsselbereiche des Gesetzes

1. Risikomanagement:
   - Verhältnismäßige Maßnahmen zur Beherrschung von Netz- und Informationssystem-Risiken
   - Orientierung an internationalen Standards wie ISO/IEC 27000

2. Berichtspflichten:
   - Verpflichtung zur Meldung erheblicher Sicherheitsvorfälle innerhalb von 24-72 Stunden
   - Informationsweitergabe an betroffene Dienstempfänger und Öffentlichkeit

3. Registrierungspflicht:
   - Alle wesentlichen und wichtigen Einrichtungen müssen sich bei der Stabsstelle Cyber-Sicherheit registrieren

Besonderheiten

Fokus auf Zusammenarbeit zwischen öffentlichen und privaten Akteuren

Klare Verbindungen zur EU-NIS-2-Richtlinie und anderen EU-Regelwerken

Organisatorische Umsetzung

Stabsstelle Cyber-Sicherheit:

- Nationale Behörde für Cybersicherheitsaufsicht
- Führt Register, koordiniert Meldungen und gewährleistet grenzüberschreitende Zusammenarbeit

5 Schlüsselmaßnahmen

Um **NIS2-compliant** zu sein, sollten Organisationen die folgenden fünf Schlüsselmaßnahmen umsetzen:

1. **Risiko- und Schwachstellenanalyse**
2. **Implementierung robuster Cybersecurity-Maßnahmen**
3. **Incident-Response- und Notfallpläne erstellen**
4. **Reporting und Informationsaustausch**
5. **Sensibilisierung und Schulung der Mitarbeiter**

Acronis

Acronis Cyber Protect Cloud-Plattform

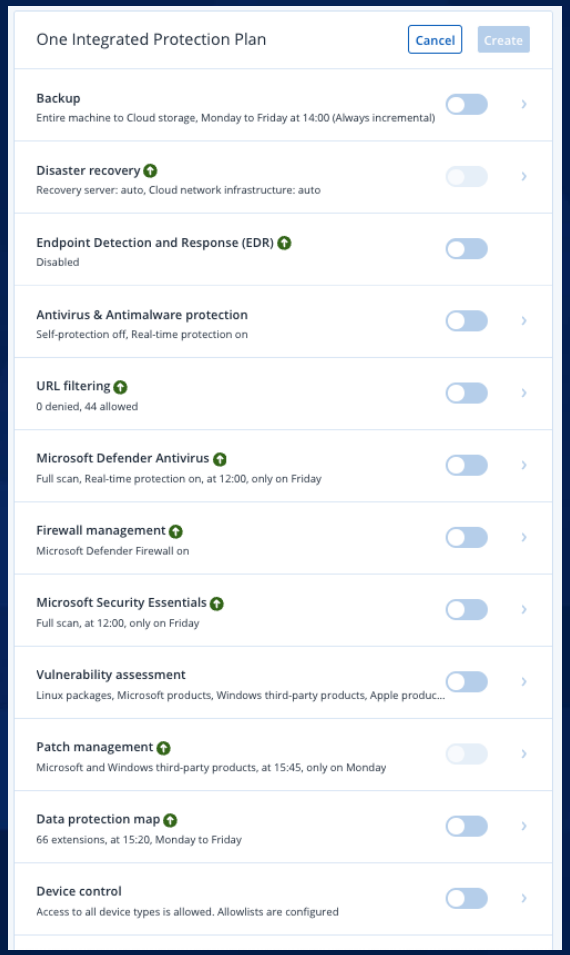
#CyberFit

Die Kraft der nativen Integration

Integration auf allen Ebenen: Management, Services, Technologie

- ✓ Beseitigung der Komplexität
- ✓ Bereitstellung neuer automatisierter Sicherheitsfunktionen
- ✓ Verwalten Sie alles von einer Konsole aus
- ✓ Kosten niedrig halten
- ✓ Effiziente Support-Eskalation mit einem Anbieter

Eine Agent • Regel • UX/UI • Lizenz • Anbieter



Native Integration

Benutzerfreundlichkeit

Ein einziger Agent, eine einzige Konsole und eine einzige Richtlinie für alle Dienste sowie ein einziges Dashboard für die Überwachung

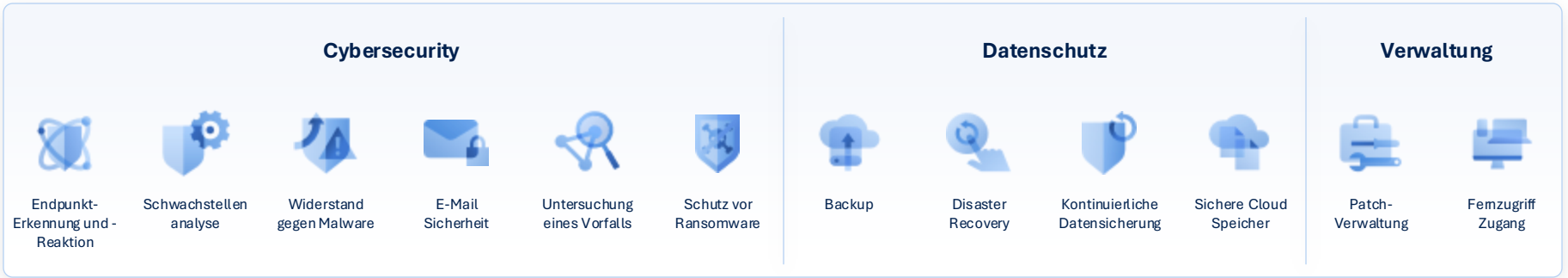
Operative Effizienz

Massenverwaltung in Umgebungen mit mehreren Mandanten, die für eine verteilte, vielfältige Kundeninfrastruktur konzipiert sind

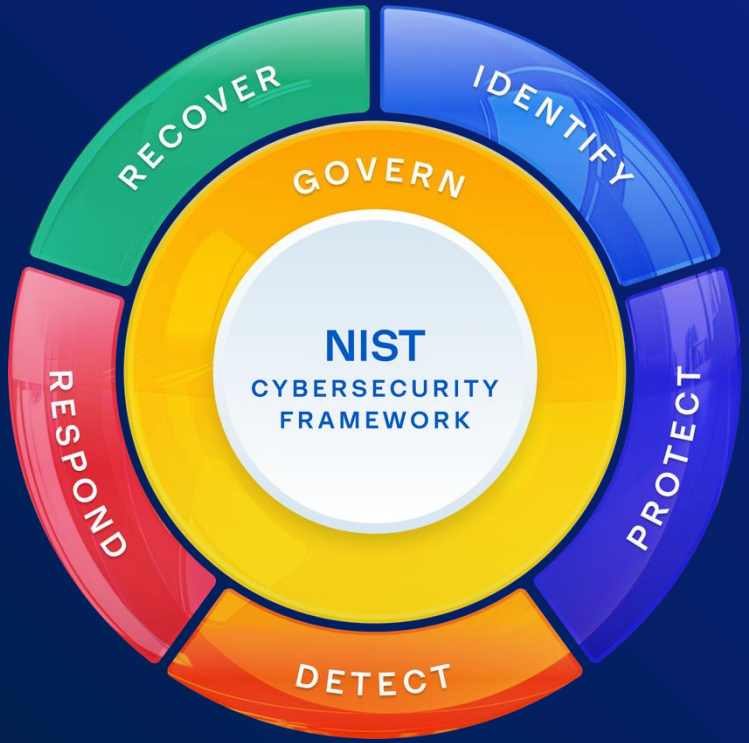
Plattform für die Integration

Erweiterbare und anpassbare Plattform zur Integration aller IT-Tools in einen einzigen Technologie-Stack

Integrierte Cybersicherheit, Datenschutz und Verwaltung in einer einzigen Lösung



Acronis Cyber Protect: Vollständige Abdeckung des NIST-Frameworks



Govern

- Provisioning via a single agent and platform
- Centralized policy management
- Role-based management
- Information-rich dashboard
- Schedulable reporting

Identify

- Software and hardware inventory
- Unprotected endpoint discovery
- Content discovery
- Data classification
- Vulnerability assessments

Protect

- Security configuration management
- Patch management
- Device control
- Data loss prevention
- Security training

Detect

- AI- and ML-based behavioural detection
- Exploit prevention
- Anti-malware and anti-ransomware
- Email security
- URL filtering

Respond

- Rapid incident prioritization
- Incident analysis
- Workload remediation with Isolation
- Forensic backups
- Remote access for investigation

Recover

- Rapid rollback of attacks
- One-click mass recovery
- Self-recovery
- Backup integration
- Disaster recovery Integration

So könnte Acronis konkret helfen (nicht nur NIS2 & CSG)

Pflichten gem. NIS2	**Acronis Cyber Protection**
Risikomanagement und -bewertung	Globale Bedrohungsüberwachung und intelligente Alarmmeldungen (über die Acronis SOC), Software- und Hardware-Inventarisierung, Autodiscovery neuer Workloads, #CyberFit-Score
Incident-Management (Bewältigung von Sicherheitsvorfällen)	Cyber Security + EDR/XDR, Email Security, Collaboration App Security
Aufrechterhaltung des Betriebs	Überwachung der Laufwerksintegrität, Cyber Scripting, Data Protection-Karte, Kontinuierliche Datensicherung (CDP), Remote Access
Notfallwiederherstellung	Safe Recovery, Bare Metal Recovery, Disaster Recovery, One Click Recovery
Sicherheit der Lieferkette	Cyber Security + EDR/XDR, Forensik Backups, URL Filterung
Schwachstellen-Management	Schwachstellen Bewertung und Patch-Verwaltung (automatisiert), SmartDeploy (Softwareverteilung)
Notfallkommunikation	Monitoring und Berichterstattung, Integration in kundenspezifische Systeme, API
Schulungen	Automatisierte Awarness Trainings mit Phishing-Simulation

Acronis sicherheitsrelevante Zertifizierungen

FIPS 140-2

Acronis AnyData Cryptographic Library has been successfully verified by NIST

ISO 27001

Acronis has Information Security Management System in accordance with standard ISO 27001:2013.

GDPR

Acronis is GDPR compliant through self-assessment as of May 25, 2018.

ISO 9001

Compliant with ISO 9001:2015

GLBA (Gramm-Leach-Bliley Act)

GLBA is applicable to financial institutions, compliant to Title V, Subtitle A, Section 501.(b)

TAA

Acronis products are “TAA compliant” as manufactured or “substantially transformed” in Switzerland

HIPAA

An independent third party gap analysis, showing that Acronis is compliant with HIPAA rules

Privacy Shield

Acronis is EU-US and Swiss-US Privacy Shield certified

Acronis Cyber Protect

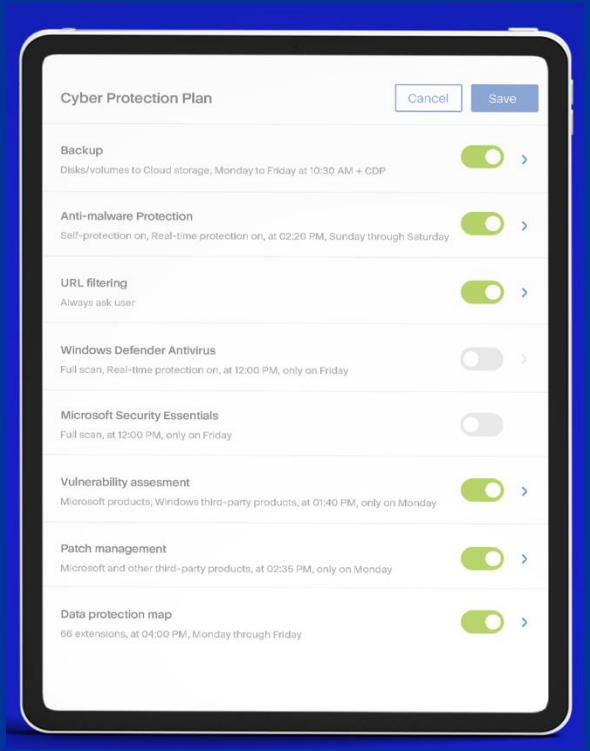
- Ein Tool für Cyber Protection
- Verwaltung mehrerer Kunden/Standorte
- Automatisierung und native Integration
- Einhaltung lokaler Vorschriften (Compliance)
- Begrenzte Budgets, Ressourcen und Zeit

Umfassende integrierte Funktionen

A NIS2

Business Mgmt.		Backup and Disaster Recovery					Cybersecurity							
														
Remote Monitoring Access (RMM)	Patch Management	Trad. Backup	Backup as a service	Archive as a service	Disaster Recovery as a service	Data visibility	Data Loss Prevention	Incident investigation	Ransomware protection	Vulnerability assessment	Detection & response	Endpoint protection	Malware Resistance	Messaging Security

... über eine einfach zu bedienende Oberfläche...



← Zurück zur Ressourcenbibliothek

Service Provider

Whitepaper

NIS-2-Briefing für MSPs

Andere Sprachen English Español (ES) Français Italiano

Was bedeutet NIS 2 für Service Provider in der EU

Das Ziel der Richtlinie über Netz- und Informationssysteme (NIS) „... war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen."

Während die NIS-Richtlinie eine wichtige Rolle bei der Gestaltung der Cybersicherheitsverfahren innerhalb der EU gespielt und international für Aufmerksamkeit gesorgt hat, hat ihre erfolgreiche Umsetzung auch die Cybersicherheitsrichtlinien in Ländern außerhalb der EU beeinflusst. Da Unternehmen, die in der EU tätig sind, unabhängig von ihrem Hauptsitz Compliance-Vorschriften einhalten müssen, haben viele Einzelunternehmen, für die diese Richtlinie gilt, die vorgeschriebenen Cybersicherheitspraktiken gleich auf ihre gesamte Organisation übertragen.

Am 17. Oktober 2024 tritt eine neue, überarbeitete NIS-Version, NIS 2, in Kraft.3 Angesichts der breiten Akzeptanz innerhalb der EU und des großen Einflusses über die EU-Grenzen hinaus ergeben sich aus der Neuauflage der Richtlinie wichtige Compliance-Auswirkungen für Managed Service Provider (MSPs), IT Service Provider und deren Kund:innen.

Acronis

Thank you! We appreciate your interest.

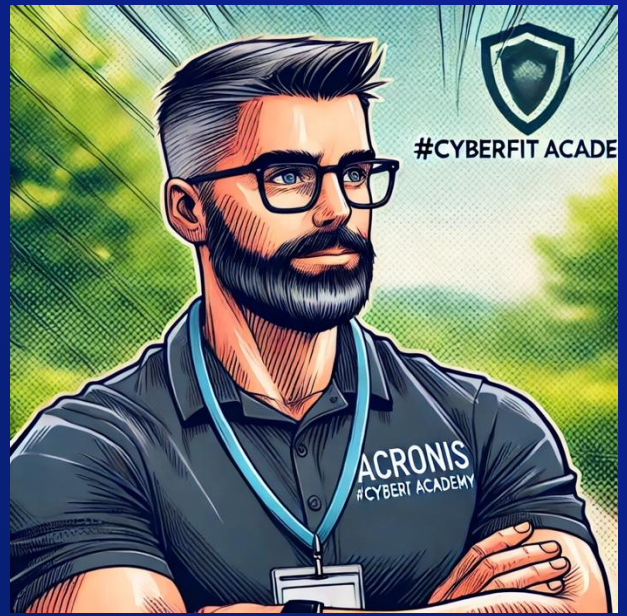
Genießen Sie Ihr kostenloses whitepaper Klicken Sie auf die untenstehende Schaltfläche Jetzt lesen um das Whitepaper einzusehen.

Jetzt lesen

Acronis

Vielen Dank!

markus.bauer@acronis.com



#CyberFit