ISL Member of the DTS Group

ISL
NIS2 & DTS COCKPIT

Compliance-Anforderungen erfolgreich & nachhaltig umsetzen, mit DER 24/7 Security Operations Plattform.

1. WAS IST NIS2?

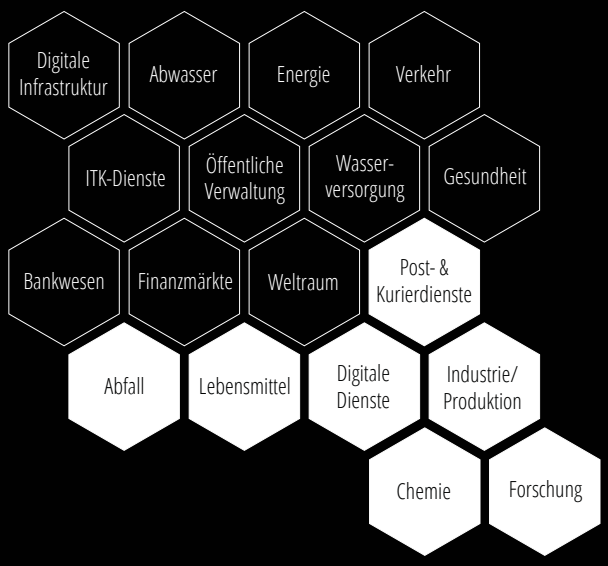
- Eine neue EU-weite Richtlinie zum Schutz von Netzwerk- & Informationssystemen
- Dient, zusammen mit der EU-DSGVO, der Steigerung der IT-Sicherheit in der EU

2. AB WANN GILT NIS2?

- Januar 2023 in der EU in Kraft getreten
- Bis Oktober 2024 wird die Richtlinie in nationales Recht überführt, ab dann gelten verpflichtende Sicherheitsmaßnahmen

3. FÜR WEN GILT NIS2?

- Für Unternehmen mit min. 50 Beschäftigten oder min. 10 Mio. € Jahresumsatz & Jahresbilanzsumme
- Außerdem müssen Unternehmen zu einem dieser 18 betroffenen Sektoren gehören:



4. ANFORDERUNGEN GEMÄß NIS2:

- Asset Management
- Aufrechterhaltung des Betriebs (Business Continuity)
- Dokumentationspflichten
- Konzepte für Maßnahmen
- Meldepflichten, Sanktionen & Haftung im Fall eines Incidents
- Regelmäßige Sicherheitsaudits & -tests
- Schulungen & Trainings
- Sicherheit der Lieferkette (Supply Chain Security)
- Vorfallsmanagement

5. NOTWENDIGE MAßNAHMEN ZUR STÄRKUNG DER IT:

- Business Continuity: Backup Management, Disaster Recovery, Krisenmanagement
- Effektivität: Vorgaben zur Messung von Cyber- & Risikomaßnahmen
- Einkauf: Sicherheit in der Beschaffung von IT- & Netzwerksystemen
- Incident Management: Prävention, Detektion & Bewältigung von Sicherheitsvorfällen
- Kommunikation: Sicherer Sprach-, Video- & Textaustausch
- Kryptographie: Verschlüsselung, wo immer möglich
- Policies: Richtlinien für Risiken & Informationssicherheit
- Supply Chain: Sicherheit in der Lieferkette
- Zugangskontrolle: Einsatz von MFA & SSO

Mit dem DTS Cockpit helfen wir Ihnen maßgeblich bei den notwendigen Maßnahmen!

6. DIESE DTS COCKPIT FEATURES UNTERSTÜTZEN SIE BEI DER ERFÜLLUNG VON ANFORDERUNGEN BZGL. NIS2, KRITIS & NIST:

- Incident Management: 24/7 Erkennung, Analyse, Eindämmung & Reaktion auf Sicherheitsvorfälle in EINER Lösung
  - Die Erfüllung der Meldepflicht mit Frühwarnung, Bericht & daraus resultierenden Abhilfemaßnahmen können über das DTS Cockpit umgesetzt werden
  - Proaktiver Ansatz, indem potenzielle Sicherheitslücken erkannt werden, bevor Angreifer sie ausnutzen können
- Policies
  - Objektive Risikoeinschätzung & kontinuierliche Bewertung Ihres Sicherheitslevels
  - ARP-GUARD als NAC inklusive: Endgeräte & Störquellen werden sichtbar & lassen sich gezielt lokalisieren. Anhand dieser Transparenz können individuelle Compliance-Policies hinterlegt & durchgesetzt werden.
- Business Continuity: Geschäftskontinuität sichern mit dem passenden DTS Incident Response Service & dem erfahrenen Krisenmanagement der DTS
- Regelmäßige Sicherheitsaudits & Penetrationstests: wiederkehrendes Testing & Re-Testing der gesamten Umgebung durch kontinuierliche, individuell abgestimmte Assessments
- Effektivität der Risikomanagement-Maßnahmen
  - Aufbau & regelmäßige Bewertung der Wirksamkeit von Risikomanagement-Maßnahmen mit kontinuierlicher Überprüfung durch das DTS Purple Teaming
  - DTS Cockpit versteht Cyber Security als ganzheitlichen, fortwährenden Prozess
- Cyber-Hygiene (z. B. Updates): Device Compliance durch den DTS Client
- Mehr IT-Sicherheit im Allgemeinen: aus eigenen, zertifizierten & EU-DSGVO konformen Rechenzentren bereitgestellt

SEHEN, VERSTEHEN, AGIEREN, VALIDIEREN & OPTIMIEREN ALS ALL-IN-ONE

DTS Cockpit ist DER essenzielle Baustein einer durchgängigen Sicherheitsarchitektur: vollständige Transparenz über angebundene Sicherheitslösungen, aktive Steuerungsmöglichkeit zur Reaktion auf Vorfälle, ein zentraler Status Ihrer Sicherheitsinfrastruktur und -Services.

PROVIDING THE MISSING LINK

Das Purple Teaming des DTS Cockpits besteht aus erfahrenen SOC-Analysten (Blue Team) und zertifizierten IT-Sicherheitsexperten (Red Team) und bietet einen einzigartigen Ansatz. Denn mit dieser Kombination steht Ihnen DTS als kontinuierlicher „Trainer“ mit Rat und Tat zur Seite und verbessert nachhaltig Ihre präventive Sicherheitsinfrastruktur.

EASY TO USE. EASY TO PAY.

Unser transparentes Preismodell folgt dem Grundsatz „vom Mittelstand für den Mittelstand“. Die Lösung ist eine 24/7/365 ganzheitliche Cyber-Security-Strategie, welche einen Enterprise Service bereitstellt und trotzdem für Unternehmen jeder Größe bezahlbar ist.

ISL Internet Sicherheitslösungen GmbH
+49 234 976672-0

isl.de
info@isl.de