MACONIA

IKT-Sicherheitskonferenz 2024

Wien, 18. September 2024

Heute NIS2 - Morgen NIS3 – wie gut geschützt sind wir wirklich?

Zur Person

Bundesakademie für Sicherheitspolitik

30 Jahre
VERNETZT DENKEN, GEMEINSAM HANDELN

Fachwerkstatt Sicherheit

MACONIA

Björn Hawlitschka

- Diplom-Politologe
- Projektleiter an der Bundesakademie für Sicherheitspolitik
- Leiter des Schaltkreis beim Informationsbüro für Wirtschaftssicherheit
- Gründer der Fachwerkstatt Sicherheit
- Manager bei der MACONIA GmbH

Worum geht es?

Cybersecurity Richtlinie der europäischen Union

- Richtlinie muss bis 17 Oktober 2024 in nationales Recht umgewandelt werden
- Umsetzung in Deutschland erfolgt mit NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz

Was ist neu?

- Erweiterung der Sektoren: Important Entities, Essential Entities
- Betroffene Betreiber: ab 50 Mitarbeitenden/10 Mio. EUR Umsatz
- Anforderungen steigen und Cyber Security muss in Lieferketten betrachtet werden
- Zusammenarbeit zwischen Betreibern und Behörden wurde vertieft
- Maximalstrafen erhöht auf bis zu 10 Mio. Euro, je nach Sektor

Ziele von NIS-2

- Erhöhter Schutz gegen Cyberbedrohungen gegenüber kritischen Infrastrukturen und betroffenen Organisationen
- Schaffung eines hohen EU-weiten Sicherheitsniveaus

Warum NIS-2?

- NIS-1 war zu abstrakt und wurde nicht einheitlich in der EU umgesetzt
- Kritische Infrastrukturen in einzelnen Ländern waren unterschiedlich eingestuft
- Keine Regelung bzgl. der Überwachung von Umsetzungen und fehlende gemeinsame Krisenreaktionen

Für wen gilt es?

1

Kriterium:

Für Unternehmen mit

- Mindestens 50 Mitarbeitenden UND
- Einem Jahresumsatz/Bilanz von über 10 Mio. Euro

2

Kriterium:

Der Unternehmenssektor zusätzlich zu der Unternehmensgröße (wenn das Unternehmen in einem von der NIS2 definiertem KRITIS-Sektor tätig ist)

3

Kriterium:

Wenn das Unternehmen der alleinige Anbieter eines gemäß NIS2 wesentlichen oder kritischen Dienstes ist (ungeachtet der Größe)

➢ Wird **eines von drei** Kriterien erfüllt, fällt eine Einrichtung unter die NIS-2-Richtlinie.

Nicht nur für Wichtigtuer

„Besonders wichtige betroffene Einrichtungen“:

- Proaktive Aufsicht
- Geldstrafen bei Verstößen (bis zu 10 Mio. € oder 2% des weltweiten Vorjahresumsatzes)

„Wichtige betroffene Einrichtungen“:

- Reaktive Aufsicht
- Geringere Geldstrafen bei Verstößen (bis zu 7 Mio. € oder 1,4% des weltweiten Vorjahresumsatzes)

Nicht nur für Wichtigtuer

„Besonders wichtige betroffene Einrichtungen“:

- Proaktive Aufsicht
- Geldstrafen bei Verstößen (bis zu 10 Mio. € oder 2% des weltweiten Vorjahresumsatzes)

„Wichtige betroffene Einrichtungen“:

- Reaktive Aufsicht
- Geringere Geldstrafen bei Verstößen (bis zu 7 Mio. € oder 1,4% des weltweiten Vorjahresumsatzes)

Ja, aber - Ausnahmeregelungen

MACONIA

- Unternehmen mit weniger als 50 Mitarbeitern oder einem Jahresumsatz unter 10 Millionen Euro (es sei denn das U. ist alleiniger Anbieter eines kritischen Dienstes)
- Unternehmen die kritischen Tätigkeiten nachgehen oder mit Systemrisiken und grenzüberschreitenden Auswirkungen verbunden sind, können in den Anwendungsbereich fallen, selbst wenn sie weniger als 50 Mitarbeiter haben oder der J.U. unter 10 Mio.€ liegt
- Einrichtungen in den Bereichen Verteidigung, nationale Sicherheit, öffentliche Sicherheit, Strafverfolgung sowie Justiz, Parlamente und Zentralbanken

Alles kann, NIS muss – sonst Strafe

Besonders wichtige Sektoren

10 Mio. €

oder

2%

des weltweiten Jahresumsatzes sofern >500 Millionen €

Auswahl erfolgt je nachdem, welcher Betrag höher ist

Besonders wichtige betroffene Einrichtungen:

- Energie
- Verkehr
- Bankwesen
- Finanzmarkt-infrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- öffentliche Verwaltung
- Weltraum

Wichtige betroffene Einrichtungen:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/ Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Alles kann, NIS muss – sonst Strafe

MACONIA

Wichtige Sektoren

7 Mio. €

oder

1,4%

des weltweiten Jahresumsatzes
sofern >500 Millionen €

Die Höhe der Strafe ist somit

vergleichbar mit der DSGVO

Wichtige betroffene Einrichtungen:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/ Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Besonders wichtige betroffene Einrichtungen:

- Energie
- Abwasser
- Verkehr
- Digitale Infrastruktur
- Bankwesen
- Verwaltung von IKT-Diensten (B2B)
- Finanzmarkt-infrastrukturen
- öffentliche Verwaltung
- Gesundheitswesen
- Weltraum
- Trinkwasser

Trotz allem - es lohnt sich!

MACONIA

Schätzung des Umsetzungsaufwands

(BMI)

1,5 Mrd. €

für die primär betroffenen 27.000 Unternehmen.

Schaden durch Cybercrime im Jahr aktuell

(BITKOM)

206 Mrd. €

davon 11 Mrd. € Schaden durch Ransomware.

19. Juli 2024 – kein Sommermärchen

Foto: https://assets.chaos.social/cache/media_attachments/files/112/812/257/953/926/994/original/c9de6459751f2ebf.png

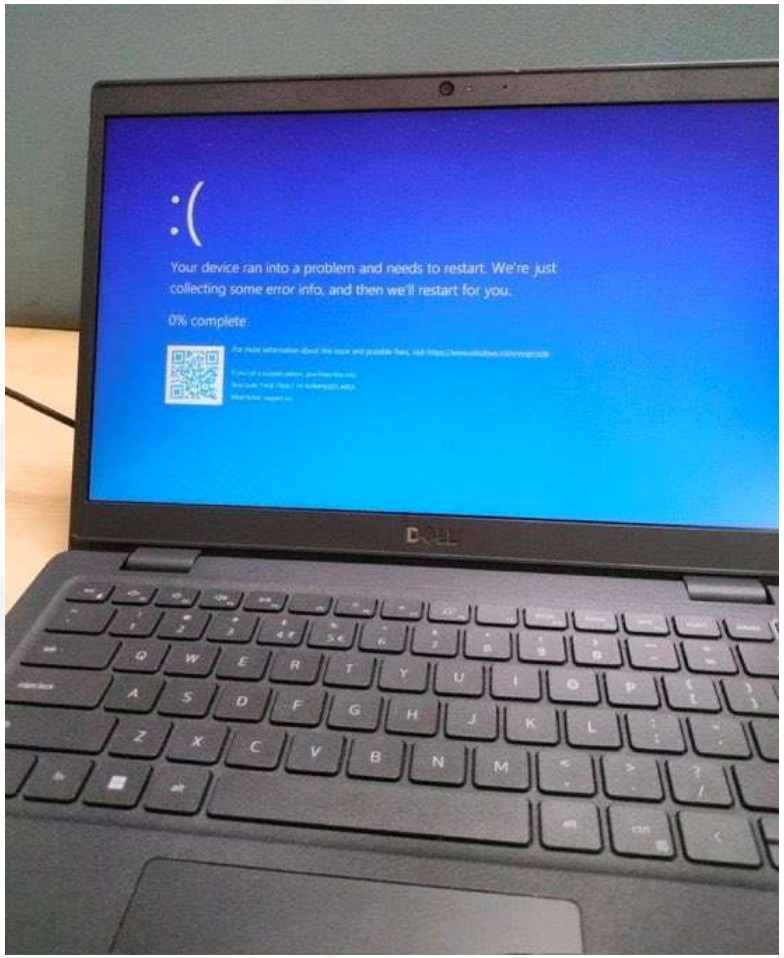
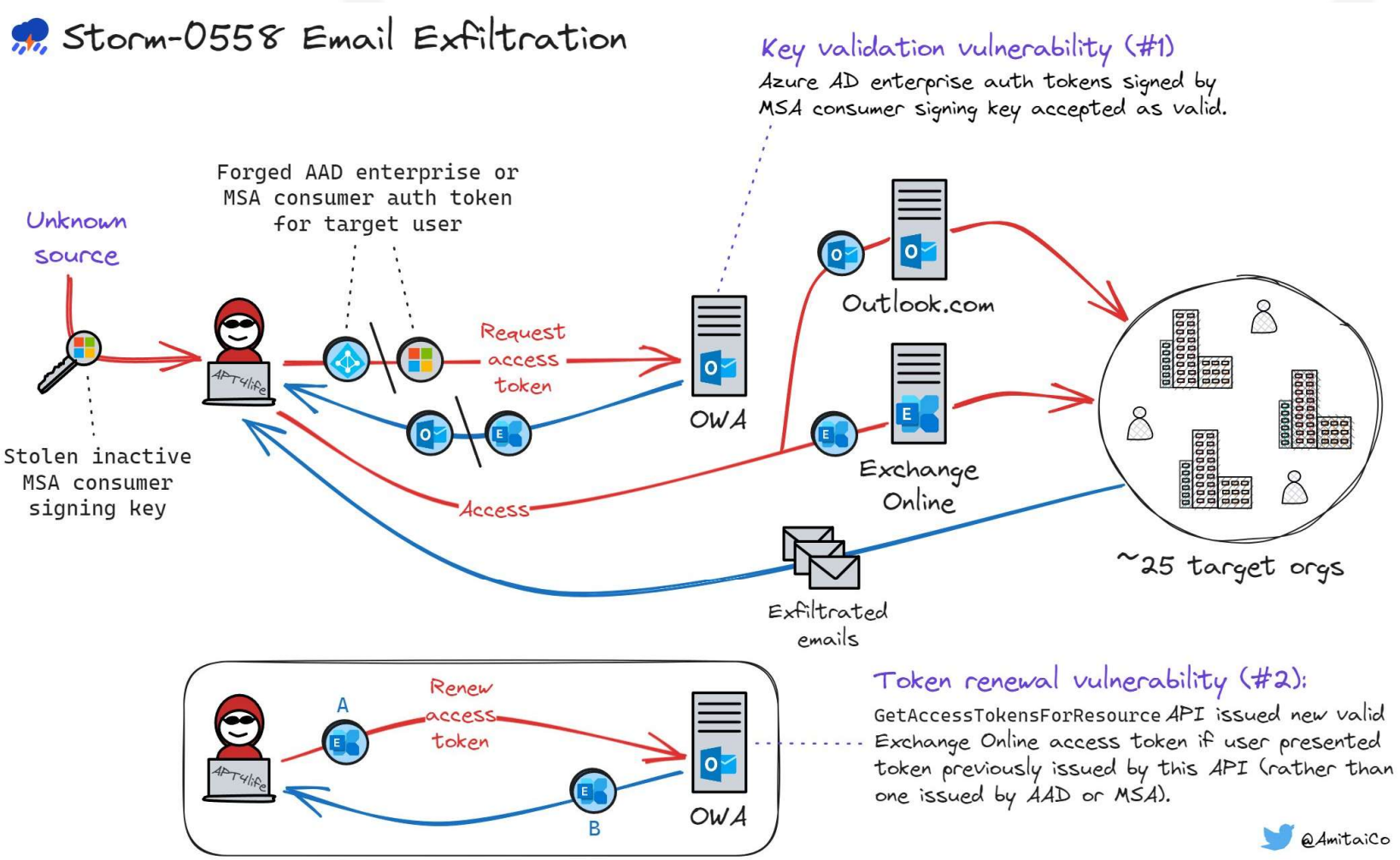


Foto: https://x.com/SoloSatoshi/status/1814278313919103289

Microsoft – der Elefant im Raum

Foto: https://twitter.com/AmitaiCo/status/1680955485463852817?s=20



Vielen Dank für Ihre Aufmerksamkeit

MACONIA