NOVEMBER 2025

NEWSLETTER °2

GO CLOUD GO SECURE

Co-funded by the European Union

🚀 Say Hello to Go Cloud! Go Secure!

Liebe Leser:innen,
wir freuen uns, Sie wiederzusehen!

Sie lesen gerade den zweiten Newsletter unseres Projekts „Go Cloud! Go Secure! “.

Seit unserem letzten Newsletter ist viel passiert! Wir haben unsere CSI-Matrix getestet und fertiggestellt, uns persönlich in der wunderschönen Stadt Sofia in Bulgarien getroffen und uns intensiv mit der Entwicklung der Go Cloud-Schulungsmaterialien beschäftigt.

Diese Ausgabe enthält viele nützliche Ressourcen und Informationen, mit denen Sie Ihre Cybersicherheit weiter verbessern können.

Vielen Dank, dass Sie uns begleiten!
Das Go Cloud-Team

Highlights

Eine Nachricht des Go Cloud! Team
- Seite 1

Interne und Externe Evaluierung der CSI Matrix
-Seite 2

The Matrix is Ready!
-Seite 3

Transnational Partner Meeting in Sofia
-Seite 4

Projekte zu Cybersecurity-Themen
-Seite 5

Cybersecurity Fun Facts
- Seite 6

INTERNE UND EXTERNE EVALUIERUNG DER CSI MATRIX

Im Rahmen von WP2–A5 „Test, Bewertung und Verfeinerung der digitalen CSI-Matrix" führten die Partner Praxistests durch, um zu überprüfen, wie nützlich, klar und benutzerfreundlich die Cloud Security Implementation (CSI)-Matrix ist.

Internal Testing

Für die internen Tests probierten Mitarbeiter:innen von Partnern, die nicht an der Entwicklung der Matrix beteiligt waren, diese aus und gaben frisches und unvoreingenommenes Feedback. Sieben Personen mit einschlägiger Erfahrung nahmen daran teil, von denen die meisten zuvor mit Cloud-Sicherheitstools gearbeitet hatten. Sie fanden die vorgeschlagenen Schwachstellen und Abhilfemaßnahmen angemessen und schätzten den praktischen Wert des Tools. Die meisten Tester sagten, die Matrix sei intuitiv und einfach zu bedienen, und sie schätzten insbesondere das farbcodierte Risikosystem. Das Feedback war insgesamt sehr positiv: Die Matrix wurde als übersichtlich, gut strukturiert und gut auf die Bedürfnisse von KMU abgestimmt empfunden. Alle internen Tester gaben an, dass sie das Tool nutzen und weiterempfehlen würden.

External Testing

Auch die externen Tests verliefen sehr gut. Alle Partner sammelten Beiträge von einer breiten Mischung aus KMU-Mitarbeitern, IT-/Cloud-Sicherheitsexperten, Berufsausbildern und anderen Fachleuten. Die Gruppe war fast gleichmäßig zwischen Personen mit und ohne Vorkenntnissen im Umgang mit Cloud-Sicherheitstools aufgeteilt, was eine ausgewogene Perspektive ermöglichte. Die Teilnehmer empfanden die Matrix als klar strukturiert, relevant und detailliert auf dem richtigen Niveau.Sie bestätigten, dass die Zuordnungen von Schwachstellen und Abhilfemaßnahmen sinnvoll sind, und empfanden die Matrix sowohl für die praktische Arbeit als auch für Schulungen als nützlich. Über 90 % gaben an, dass sie sie beruflich nutzen und weiterempfehlen würden.

THE MATRIX IS READY!

AVAILABLE NOW

ENTDECKEN SIE DIE CSI MATRIX UND SICHERN SIE IHRE CLOUD INFRASTRUKTUR!

Wir freuen uns, Ihnen mitteilen zu können, dass die Cloud Security Implementation Matrix, das erste Ergebnis des Erasmus+-Projekts „Go Cloud! Go Secure!“, nun auf der Projektwebsite verfügbar ist.
Die CSI-Matrix richtet sich in erster Linie an KMU, die Cloud-Dienste nutzen oder deren Nutzung in Betracht ziehen, aber möglicherweise nicht über eigene Sicherheitsteams oder Cloud-Sicherheitsexpertise verfügen.
Das Tool ist einfach, flexibel und KMU-freundlich gestaltet, ohne zu viel Fachjargon zu verwenden, und unterstützt Unternehmen, die Cloud-Lösungen verantwortungsbewusst einsetzen und gleichzeitig die Sicherheit gewährleisten möchten.
Die KMU müssen lediglich das Cloud-Modell auswählen, auf das sie sich verlassen, und die Matrix zeigt, bewertet und mindert die mit dem ausgewählten Cloud-Modell verbundenen Risiken.

Die CSI-Matrix funktioniert in vier einfachen Schritten:

1. Wählen Sie das Cloud-Service-Modell aus, das Sie verwenden oder verwenden möchten (z. B. SaaS, PaaS, IaaS).
2. Anhand Ihrer Auswahl können Sie die für Ihre Cloud-Umgebung relevantesten Sicherheitsrisiken überprüfen.
3. Die Matrix bewertet das Risikoniveau, das jede Bedrohung für Ihr Unternehmen darstellt – das bedeutet, dass sie Prioritäten setzt, die für Ihr Unternehmen am wichtigsten sind.
4. Als letzten Schritt erhalten Sie klare Ratschläge und Tipps, die sich am bekannten OWASP Top 10-Framework orientieren.

Am Ende des Prozesses kann ein personalisiertes PDF mit allen Ergebnissen und Empfehlungen heruntergeladen werden. Neben Englisch ist das Tool in fünf weiteren europäischen Sprachen verfügbar.

TRANSNATIONAL PARTNER MEETING #2

16-17 October 2025, Sofia

Das Projekt „Go Cloud! Go Secure!“ hielt kürzlich sein zweites internationales Treffen in Sofia, Bulgarien, unter der Leitung von Acta Consulting ab. Partner aus Ungarn, Italien, Österreich und Zypern kamen zusammen, um die Fortschritte zu überprüfen und die nächsten Schritte zu planen.

Ein wichtiges Ergebnis des Projekts, die Cloud Security Implementation (CSI) Matrix, ein digitales Selbstbewertungstool, wurde gründlich getestet. Während des externen Pilotprojekts gaben 38 Fachleute aus fünf Ländern Feedback, wobei 100 % das Tool weiterempfehlen würden. 81,1 % fanden die Logik der Risikobewertung „sehr nützlich”, und die Teilnehmer bestätigten die stabile Leistung des Tools. Interne Tests mit sieben Mitarbeitern unterstrichen ebenfalls den Wert des Tools, wobei nur geringfügige Vorschläge zur Benutzerfreundlichkeit gemacht wurden.

In der nächsten Phase wird das Arbeitspaket 3 das CSI-Implementierungsmodell in fünf Schritten liefern:

- Analyse (Service-Inventar, Risikokarte, Compliance)
- Definition (Richtlinien, Rollen, Ziele)
- Planung (Maßnahmen, Schulungen)
- Implementierung (technische Schritte, Sensibilisierung)
- Verifizierung (Tests, Feedback)

Das CSI-Modell hilft KMU bei der Einführung sicherer Cloud-Systeme, indem es sie durch die Risikoidentifizierung, Sicherheitsmaßnahmen und den laufenden Schutz führt. Dieser Ansatz erhöht die digitale Bereitschaft, reduziert Cyberrisiken und stärkt das Vertrauen der Kunden.

Mit Blick auf die Zukunft wird das Arbeitspaket 4 Schulungsmaterialien bereitstellen, darunter einen Fragebogen zur Vorabbewertung, einen CSI-Kurslehrplan und ein Online-Portal. Der Lehrplan wird noch in diesem Jahr verfügbar sein, und Anfang 2026 werden Mikro-Lernvideos auf der Grundlage realer Geschäftsbeispiele hinzukommen.

PROJEKTE ZU CYBERSECURITY - THEMEN

🚀 Cybersicherheits-schulung zur Widerstandsfähigkeit von Betriebstechnologien

https://csector.eu/

CSecTOR stattet KMU in der Fertigungsindustrie und anderen kritischen Infrastruktursektoren mit OT-Cybersicherheitsfunktionen aus.
Der Schwerpunkt liegt auf der Identifizierung von Schwachstellen, der Implementierung von Schutzmaßnahmen und der Entwicklung von Notfallplänen für Betriebstechnologiesysteme.
Das Projekt liefert eine maßgeschneiderte Methodik, ein Selbstbewertungstool und eine gemischte + E-Training-Plattform, um die Widerstandsfähigkeit in Sektoren wie Chemie, Kunststoffe, Textilien, Versorgungsunternehmen, Öl und Gas sowie Transport zu stärken.

CSecTOR

🚀 Gemeinsame Initiative zur Entwicklung von Fachkräften, damit die europäische Industrie den Mangel an Cybersicherheitsexperten überwinden kann

https://encrypt40.eu/

Encrypt 4.0 stärkt die Fähigkeit kleiner und mittlerer Fertigungsunternehmen, ihre Daten, Systeme und Abläufe im Umfeld von Industrie 4.0 zu schützen.
Das Projekt hilft Unternehmen dabei, Cyberrisiken zu identifizieren, zu analysieren und zu bekämpfen, und unterstützt gleichzeitig die Entwicklung qualifizierterer Fachkräfte im Bereich Cybersicherheit.
Es bietet praktische, benutzerfreundliche Tools wie die Cyber Risk Audit Matrix, ein praxisorientiertes Cybersicherheits-Schulungslabor und eine Sammlung von Fallstudien zu realen Cybervorfällen mit Abwehrstrategien.
Encrypt 4.0 fördert interaktives, projektbasiertes Lernen, befähigt KMU-Manager zur Einführung proaktiver Cybersicherheitspraktiken und fördert den Wissensaustausch, um die Widerstandsfähigkeit und digitale Bereitschaft im gesamten industriellen Ökosystem zu verbessern.

ENCRYPT 4.0

THE FASCINATING WORLD OF CYBERSECURITY

Es gibt Cyber Fischer!

Der Begriff „Phishing“ (betrügerische Versuche, an sensible Informationen zu gelangen) leitet sich von der Idee ab, einen Köder (wie eine E-Mail oder eine Website) zu verwenden, um Opfer „an den Haken zu bekommen“, ähnlich wie Fischer Köder verwenden, um Fische anzulocken.

Weitere Informationen zum Thema Phishing finden Sie in unseren Schulungsunterlagen :)

The first virus wasn’t a scam.

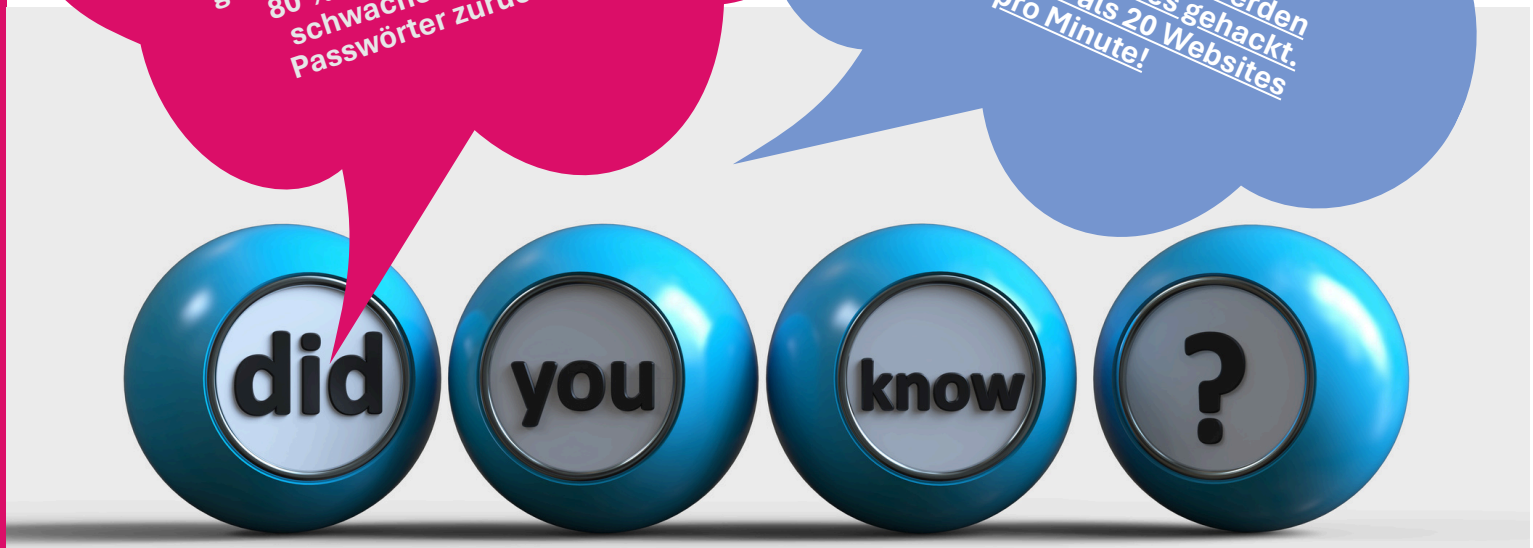
Der erste bekannte Computervirus hieß Creeper und wurde Anfang der 1970er Jahre als sich selbst replizierendes Programm entwickelt. Er richtete keinen Schaden an, sondern zeigte lediglich die Meldung „I'm the Creeper, catch me if you can!“ (Ich bin der Creeper, fang mich, wenn du kannst!) an. Es handelte sich eher um einen Proof-of-Concept als um einen böswilligen Angriff.

Passwörter sind immer noch eine große Schwachstelle

Das weltweit am häufigsten verwendete Passwort ist nach wie vor „123456“, obwohl seit Jahren vor schwachen Passwörtern gewarnt wird. Tatsächlich sind rund 80 % aller Datenverstöße auf schwache oder gestohlene Passwörter zurückzuführen.

Es gibt mehr Cyberangriffe, als Sie vielleicht vermuten.

Die durchschnittliche Anzahl der Cyberangriffe pro Tag ist erschreckend: Täglich werden rund 30.000 Websites gehackt. Das sind mehr als 20 Websites pro Minute!



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.