



Information Security Network (ISN)

innovation is our business.

Strategische Themenschwerpunkte



Industrial Data



Information Security



Business Software



- Drehscheibe für Anbieter und Bedarfsträger im Bereich Informationssicherheit und Datenschutz
- Sensibilisierung und Unterstützung von öö. Unternehmen
- Nationale und internationale Vernetzung mit und zwischen Organisationen, Clustern und Unternehmen
- Know-how Transfer und Kooperation: Initiierung und Begleitung kooperativer Projekte (CKP)
- Internationale Sichtbarkeit und Stärkung regionaler Security Industrie

Informationssicherheit ist umfangreich



Identifizieren

- Systeme kennen
- Geschäftsumfeld
- Risiken
- Rechtliche Anforderungen

Schützen

- Zutritt und Zugriffe
- Training und Schulungen
- Wartung und Aktualisierung

Erkennen

- Anomalien erkennen

Antworten

- Schnelle und passende Reaktion auf Angriff

Wiederherstellen

- Kann ich notwendige Daten wiederherstellen?
- Lerne ich aus dem Vorfall und verbessere meine Maßnahmen?

Starke Partner. Starkes Netzwerk. Das Information Security Network.



40 Partner ✓



• F&E

- FH Oberösterreich, Fakultät für Informatik, Kommunikation und Medien, Hagenberg
- Johannes Kepler Universität Linz, Institut für Netzwerke und Sicherheit
- Logistikum Steyr



• Weitere Organisationen

- Bayerischer IT-Sicherheitscluster
- DAVITS: Datenschutz Verein IT-Sicherheit
- FH Oberösterreich, Information Security Compliance Center (ISCC)
- TeleTrusT – Bundesverband IT-Sicherheit e.V.
- Wirtschaftskammer Oberösterreich





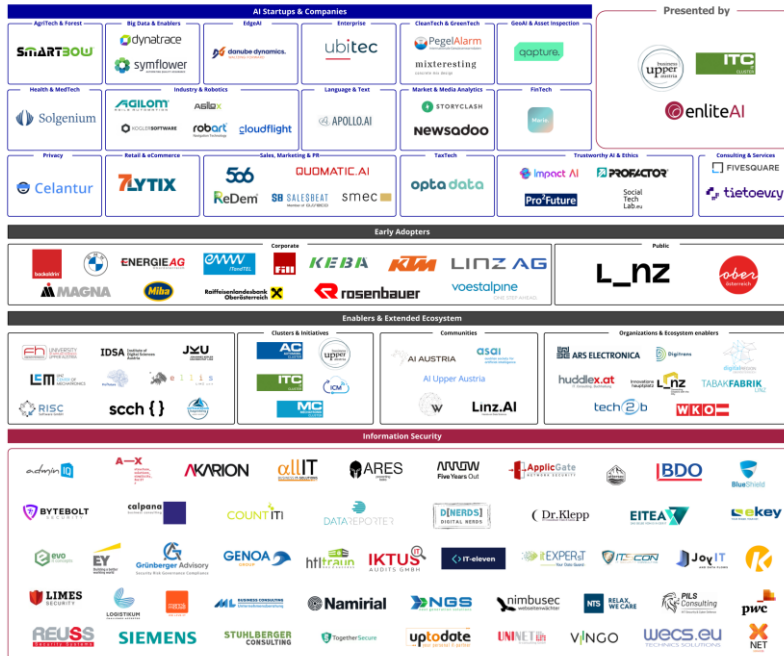
- Unterstützung der WKÖ
 - 24 h / 7 Tage
 - Erstinformation / Notfallhilfe
 - Zusätzlich kostenloses Erstgespräch mit IT-Security Unternehmen

<https://www.wko.at/Content.Node/kampagnen/cyber-security-hotline/index.html>

Update der AI & IT-Security: Landscape OÖ



AI & Information Security Landscape Upper Austria 2023



[Bericht auf unserer IT-Cluster Homepage „Wir sind die Guten“ \(itcluster.at\)](https://itcluster.at)

IT-Sicherheitshandbuch für KMU



IT-Sicherheitshandbuch für Mitarbeiter



VERHALTEN BEI IT-NOTFÄLLEN

 **Ruhe bewahren & IT-Notfall melden**
Lieber einmal mehr als einmal zu wenig anrufen!

 IT-Notfallrufnummer:

 Wer meldet?

 Welches IT-System ist betroffen?

 Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

 Wann ist das Ereignis eingetreten?

 Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten
--	--------------------------------	--

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

- [Link zur Notfallkarte](#)
- Außerdem:
 - Maßnahmenkatalog zum Notfallmanagement
 - Checkliste für Home Office
 - Cyber-Sicherheits-Check

- **hack'aware – Der KMU Security Quickcheck**
- „Schützen Sie Ihre Daten!“ Diese Aufforderung haben Sie bestimmt nicht zum ersten Mal gehört. Hackerangriffe sind eine Gefahr für alle Branchen und betreffen längst nicht mehr nur die Big Player. Gerade kleine und mittlere Unternehmen haben oft nicht die nötigen Mittel und die Manpower, um sich umfassend zu schützen.

[hack'aware – Der KMU Security Quickcheck \(digitalregion.at\)](https://digitalregion.at)

[ITC | hack'aware – KMU Security Quick Check \(togethersecure.com\)](https://togethersecure.com)

[hack'aware – Alle Maßnahmen im Überblick \(digitalregion.at\)](https://digitalregion.at)

- Chief Information Security Officer bezeichnet die Rolle des Gesamtverantwortlichen für Informationssicherheit in einer Organisation.
- Beim CISO Exchange treffen sich die Teilnehmer aus Unternehmen aller Branchen um Erfahrungen aus den Bereichen Informationssicherheit & Datenschutz auszutauschen und voneinander zu lernen.

Nächstes Treffen: [Veranstaltungen](#)

Anmeldung und Rückfragen: frederic.hadjari@biz-up.at



- Zugang zu einem maßgeschneiderten **geförderten** Schulungsangebot
- Unterstützung durch ein Beratungsteam bei Feststellung des Bildungsbedarfs und bei Erstellung eines individuellen Personalentwicklungskonzepts
- **Kostenlose** Teilnahme an Expertenvorträgen und Netzwerkveranstaltungen
- **Erfahrungsaustausch** mit anderen Unternehmen
- Der Beitritt ist kostenlos und steht weiteren Unternehmen jederzeit offen.

[Link zu allen Infos](#)



[IT-Sicherheit: TAHITI sorgt für Know-how](#)

Im Qualifizierungsseminar „Trends und Aktuelle Herausforderungen der IT-Sicherheit“ – kurz TAHITI – haben die Johannes Kepler Universität Linz, das Software Competence Center Hagenberg und Limes Security in Kooperation mit dem IT-Cluster der öö. Standortagentur Business Upper Austria und oberösterreichischen Unternehmen ein umfangreiches Weiterbildungsformat entwickelt, das optimal auf die Bedürfnisse der Betriebe abgestimmt wurde. Nach dem erfolgreichen Start im Vorjahr wird TAHITI im Frühjahr 2023 fortgeführt.

- **Kosten 2300 Euro**
- **Start: 08.03. 2024**
- **Ende: 26.04. 2024**

Förderung „Digital Starter Upgrade“



Es stehen Projekte zum Auf- u. Ausbau Digitaler Vertriebswege, Big Data-Anwendungen und die Umsetzung neuer **IT-Security Lösungen** im Mittelpunkt dieses **Förderprogramms**.

[Details zum Förderprogramm](#)





- Erste Hilfe bei Cybercrime
- Die Experten stellen rasch und unkompliziert bei allen Fragen rund um Computer- und Internetkriminalität umgehend Verhaltenstipps und Erstmaßnahmen per E-Mail zur Verfügung.
- Kontakt: against-cybercrime@bmi.gv.at

<https://bundeskriminalamt.at/news.aspx?id=3862644B6C794C4B5A42733D>



- CERT.at ist das österreichische nationale CERT (Computer Emergency Response Team).
- Gibt Warnungen, Alerts und Tipps für KMUs (kleine und mittlere Unternehmen) heraus.
- Im Falle schwerwiegender Sicherheitslücken veröffentlicht CERT.at Warnungen, um Betroffene schnellstmöglich zu informieren.

<https://cert.at/>

Entwicklung Cybercrime in Österreich

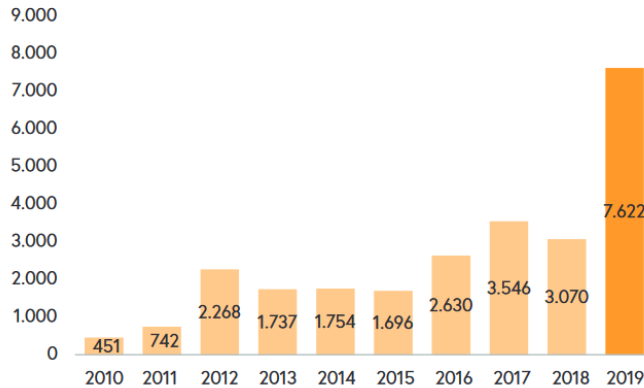
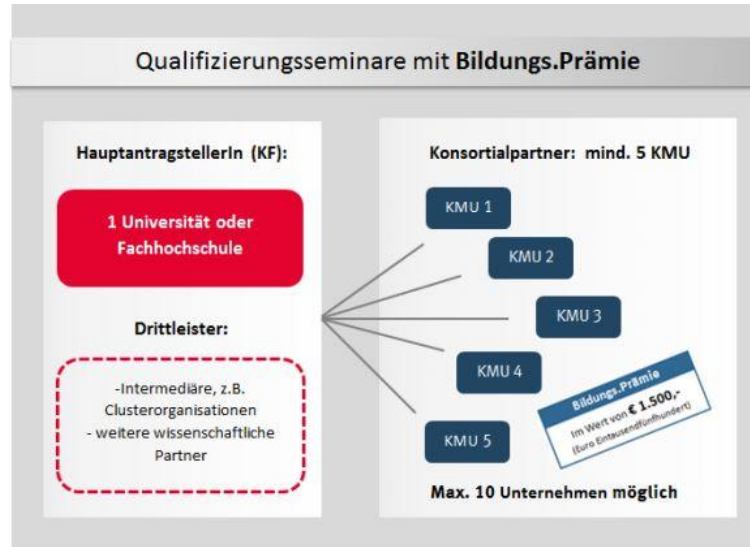


Abbildung: Entwicklung von Cybercrime im engeren Sinn in Österreich 2010 bis 2019

Die Polizeiliche Kriminalstatistik 2019: https://bundeskriminalamt.at/501/files/Broschuere_PKS_2019.pdf
[Cyber-Angriffe weltweit 2022 | KonBriefing.com](https://www.konbriefing.com)

- Die Möglichkeit gewisse Cyber-Risiken zu versichern, sollen in diesem Foliensatz aus informativen Gründen und zur Vollständigkeit erwähnt werden.
- Sind ein zusätzlicher Baustein im Risikomanagement
- Weiterführende Informationen
<https://www.wko.at/site/it-safe/cyber-versicherungen-das-risiko-einfach-auslagern.html>
- Viele Anbieter



Ein besonderer Schwerpunkt wird in der Ausschreibung auf die Themen eCommerce, **Cyber Security** und Smart Factory gesetzt

Fragen?



Frederic Hadjari

Cluster Manager
IT-Cluster OÖ

☎ +43 664 84 8 12 57

✉ frederic.hadjari@biz-up.at

🌐 www.itcluster.at/information-security-network

Business Upper Austria ist die Standortagentur des Landes Oberösterreich und Partner für Standortentwicklung, Kooperation und Förderberatung.

Diese Präsentation erhebt keinen Anspruch auf Vollständigkeit. Ziel ist die Schaffung eines groben Überblicks über ausgewählte Bereiche. Die Business Upper Austria – OÖ Wirtschaftsagentur GmbH übernimmt keine Verantwortung und Haftung für die Richtigkeit und Vollständigkeit der in dieser Präsentation enthaltenen Daten und Informationen. Jede konkrete Angelegenheit ist mit entsprechend fachkundigen Personen gesondert zu prüfen. Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung vorbehalten. Kein Teil der Foliensätze darf in irgendeiner Form ohne schriftliche Genehmigung der Business Upper Austria – OÖ Wirtschaftsagentur GmbH reproduziert, vervielfältigt oder verbreitet werden. © Business Upper Austria – OÖ Wirtschaftsagentur GmbH



innovation is our business.

info@biz-up.at, www.biz-up.at

Business Upper Austria – OÖ Wirtschaftsagentur GmbH
Hafenstraße 47-51, A-4020 Linz, T +43 732 79810

