LandesKorrespondenz
MedienInfo

I N F O R M A T I O N

zur Pressekonferenz mit

Mag. Thomas STELZER

Landeshauptmann

Markus ACHLEITNER

Wirtschafts- und Forschungs-Landesrat

FH-Prof. DI Robert KOLMHOFER

Departmentleiter Sichere Informationssysteme FH Hagenberg

Univ.-Prof. Dr. René MAYRHOFER

Vorstand Institut für Netzwerke und Sicherheit, JKU Linz

am 03. November 2022 zum Thema

„Sichere Daten – Sicherer Standort“

Ergebnisse des Expertenforums „Cyber-Security“

Impressum

Medieninhaber & Herausgeber:
Amt der Oö. Landesregierung
Direktion Präsidium
Abteilung Presse
Landhausplatz 1 • 4021 Linz

Tel.: (+43 732) 77 20-11412
Fax: (+43 732) 77 20-21 15 88
landeskorrespondenz@ooe.gv.at
www.land-oberoesterreich.gv.at

Landeshauptmann Mag. Thomas STELZER:

Oberösterreich gestaltet die Digitalisierung auch bei der IT-Sicherheit aktiv mit

„Ein wirtschaftlich starker und international exponierter Wirtschaftsstandort wie Oberösterreich steht mit seinen Produkten und Betrieben im weltweiten Rampenlicht. Dieses Rampenlicht lockt aber auch kriminelle Kräfte an. Wir erleben auch bei uns Attacken via Internet gegen unsere Betriebe, öffentliche Verwaltungen und gegen Einrichtungen der kritischen Infrastruktur. Dazu kommen Oberösterreichs Ambitionen, in Sachen Digitalisierung international eine führende Rolle einzunehmen. All das erfordert große Anstrengungen auch im Bereich der Datensicherheit“, **stellt Landeshauptmann Mag. Thomas Stelzer zum hochkarätig besetzten Expertenforum „Cyber-Security“ in Hagenberg fest, zu dem er heute gemeinsam mit Wirtschafts- und Forschungs-Landesrat Markus Achleitner eingeladen hat.**

„Wir haben heute im Softwarepark Hagenberg mit Experten und Partnern aus der Wissenschaft, den Sicherheitsbehörden und der Wirtschaft eine ganz zentrale Herausforderung im Bereich Sicherheit besprochen: Den Schutz unserer öffentlichen und betrieblichen Digital-Infrastruktur gegen zerstörerische und erpresserische kriminelle bzw. feindliche Attacken“, betont Landeshauptmann Stelzer. An diesem Expertenforum haben teilgenommen:

- FH-Prof. DI Robert KOLMHOFER - Departmentleiter „Sichere Informationssysteme“, FH Hagenberg
- Univ.-Prof. Dr. René MAYRHOFER - Vorstand Institut für Netzwerke und Sicherheit, JKU Linz
- Mag. (FH) Gert SEIDL - Leiter Cybercrime Competence Center des Bundeskriminalamtes
- Brigadier Mag. Dieter MUHR, MBA - Militärkommandant Oberösterreich
- DI (FH) Robert LAMPRECHT, MSc - Director Cyber Security & Crisis Management, KPMG
- Dr. Bernhard MARCKHGOTT, (RLB) - Präsident OÖ Kompetenzzentrum Sicheres Österreich

- Ing. Dr. Joachim HAINDL-GRUTSCH - Geschäftsführer Industriellenvereinigung OÖ
- Mag. Stefan SCHÖFL - Projektmanager Abteilung Innovationsmanagement, WKOÖ

Abwehr aktueller Gefahren und Vorbereitung auf Digitalisierung:

Wir erleben aktuell eine anhaltende Welle an krimineller Energie aus dem Internet - auch gegen Unternehmen. Zudem erleben wir insbesondere staatlich gesteuerte Angriffe auf Daten und kritische Infrastruktur in Europa. Ebenso zeichnen sich weitere neue Angriffsflächen ab:

- Wir gehen demnach in ein **Zeitalter gesteuerter gezielter Desinformationen** mit wirtschaftlichen und politischen Zielsetzungen bzw. wirtschaftlichen und politischen Absendern.
- Im **Wettlauf um Technologieführerschaft und Innovation** entstehen rund um den Erdball neue Formen der Konfliktführung. Die neuen strategischen Waffen in Wirtschaft und Machtstreben sind demnach Cyberangriffe, Spionage und die Verbreitung gezielter Fakenews.
- Zudem ist davon auszugehen, dass im Zuge der voranschreitenden Digitalisierung auch am Wirtschaftsstandort Oberösterreich **neue Systeme in Anwendung** stehen werden, die auch neue Wege der Absicherung erfordern werden.
- Ganz generell bezeichnen Zukunftsforscher **Daten als „das neue Öl der Zukunft"**. Damit sprechen die Experten **a)** einerseits die breiten Handlungsoptionen auf Basis erhobener Datenmengen an, **b)** deren wirtschaftlichen und strategischen Wert, aber auch **c)** das mit Daten verbundene Konfliktpotenzial – was umso mehr die Notwendigkeit des Schutzes von Daten und IT-Systemen unterstreicht.

„Daher wollen wir den Standort OÖ in Zusammenarbeit mit Sicherheitskräften und Wissenschaft nachhaltig und mit aller Konsequenz schützen. Hier gilt – ebenso wie für die Digitalisierung generell – für uns folgender Grundsatz: Wir wollen als Standort Oberösterreich auch die IT-Sicherheit aktiv und international mitgestalten", unterstreicht Landeshauptmann Stelzer.

Schwerpunkte im aktuellen Regierungsprogramm für Oberösterreich:

- „Oberösterreich **strebt** als führender Industrie- und Wirtschaftsstandort eine **noch stärkere Vorreiterrolle bei der digitalen Transformation** von Gesellschaft, Wirtschaft, Bildung, Gesundheitssystem und öffentlicher Verwaltung auf Gemeinde- und Landesebene an."
- „Dafür sind **digitale Infrastruktur, Fähigkeiten, Bewusstseinsbildung, Prozesse, Förderwesen, Datensicherheit, Forschung und Lehre** zentrale Erfordernisse, die in Oberösterreich konsequent gefördert und umgesetzt werden."
- „Digitalisierungsoffensive durch **Ausbau der digitalen Landesverwaltung**, um Behördenwege zu sparen und Prozesse der öffentlichen Hand effizienter zu gestalten sowie Behördenverfahren zu beschleunigen."
- „**Digitale Klassenzimmer** sollen als Basis für eine zeitgemäße Ausbildung von Kindern und Jugendlichen im Bereich der Digitalisierung dienen."
- „**Digitalisierungsoffensive in der Pflege und im Gesundheitsbereich** zur Entlastung der Mitarbeiterinnen und Mitarbeiter und zur Attraktivierung der Sozial-, Gesundheits- und Pflegeberufe."
- „Forcierung der **Förderungen zur Digitalisierung der Klein- und Mittelbetriebe** in Kooperation mit der Wirtschaftskammer Oberösterreich."

Zusammenarbeit macht Standort Oberösterreich stark und sicher:

So wird auch der Softwarepark Hagenberg gemäß dem aktuellen Regierungsprogramm sukzessive zu einem internationalen Zentrum für IT-Sicherheit ausgebaut. Weil Zusammenarbeit den Standort Oberösterreich immer ausgezeichnet und stark gemacht hat, wollen wir auch in Sachen IT-Sicherheit auf Zusammenarbeit setzen – sowohl mit dem neuen „Institute of Digital Sciences Austria" als auch mit der JKU und den Fachhochschulen sowie der oberösterreichischen Wirtschaft.

Schlussfolgerungen aus dem Expertenforum „Cybersicherheit in OÖ":

- Wir brauchen zum Schutz des Standortes OÖ die **laufende und vernetzte Bewertung von Bedrohungen** und damit eine **vernetzte Standortstrategie** im Kampf gegen Cybercrime
- Wir brauchen das klare Bekenntnis des Bundes zu **modernsten Aufklärungstechnologien** bei Polizei, Staatsschutz und militärischen Diensten.

- Wir brauchen auf Ebene der öffentlichen Verwaltung, auf Ebene der Betriebe sowie in der kritischen Infrastruktur **modernste Alarm- und Präventionspläne** im Kampf gegen Cybercrime
- Wir brauchen **neue Antworten auf neue technologische Anwendungsbereiche**: zB. 5G, Schutz des autonomen Fahrens vor Cyberattacken, Schutz Telemedizin, Schutz des Smart-Livings etc.
- Wir müssen den **Forschungsbereich Cybersicherheit stärken** und international vernetzen.
- Wir müssen die **Ausbildung von Cyber-Experten** forcieren
- Wir müssen als Standort Europa auch erkennen, dass Kampf gegen Cybercrime schon bei der Beschaffung technischer Einrichtungen sowie bei der Vergabe öffentliche Aufträge beginnt. So gesehen erfordert mehr Cybersicherheit letztlich auch die **Rückverlagerung systemrelevanter sicherheitssenibler Technologien, Produkte und Produktionsstufen nach Europa**.

Wirtschafts- und Forschungs-Landesrat Markus ACHLEITNER:

Daten sollen als das „neue Gold“ gerade in Oberösterreich besonders gut gehütet werden

„Daten sind das neue Gold und somit einer der wertvollsten Rohstoffe der digitalen Wirtschaft. Daher sind auch die Informationssicherheit und der Schutz von Daten von besonderer Bedeutung. Dies gilt in besonderem Maße für Oberösterreich, weil unser Bundesland als starker Industrie- und Wirtschaftsstandort auch ein besonders attraktives Ziel für Cyber-Attacken und digitale Erpressungsversuche ist. Zugleich will Oberösterreich die digitale Transformation aktiv mitgestalten und dabei spielt auch die IT-Sicherheit eine zentrale Rolle. Insbesondere soll unser Bundesland zu einem auch international sichtbaren Kompetenzzentrum für Cyber-Security“, **erklärt Wirtschafts- und Forschungs-Landesrat Markus Achleitner.**

„Die Voraussetzungen dafür, dass Oberösterreich zu einem Leuchtturm für IT-Sicherheit wird, sind ausgezeichnet – neben zahlreichen Unternehmen, die in diesem Bereich tätig sind, weisen vor allem auch die FH Hagenberg und die Johannes Kepler Universität Linz höchste Kompetenz in Sachen IT-Security auf. Auch das neue ‚Institute of Digital Sciences Austria‘ wird hier wichtige zusätzliche Impulse bringen“, unterstreicht Landesrat Achleitner.

Im Softwarepark Hagenberg kooperieren mehr als 75 Unternehmen sowie Ausbildungs- und Forschungseinrichtungen zum Thema IT. Rund 12 Unternehmen am Standort Softwarepark Hagenberg beschäftigen sich mit IT-Security. Dies hat zur Folge, dass sich u.a. Firmen aufgrund dieser Expertisen-Dichte im Softwarepark Hagenberg ansiedeln.

Bereits im Jahr 2000 ist mit der Gründung des ersten Studiengangs zu Computer- und Mediensicherheit die Bedeutung von Information-Security lange vor dem aktuellen Hype in Hagenberg angekommen. Durch die Absolventinnen und Absolventen stehen den Unternehmen Spezialisten mit umfangreichem Know-how zur Verfügung. Davon profitieren sowohl der Softwarepark als auch seine Kunden.

Gezielte Unterstützung für Kleine und Mittlere Unternehmen in OÖ:

„Gerade Kleine und Mittlere Unternehmen haben oft noch Nachholbedarf dabei, sich wirksam gegen Hacker-Angriffe zu schützen. Hier bietet der IT-Cluster unserer oö. Standortagentur Business Upper Austria ein umfassendes und auch niederschwelliges Angebot: Der IT-Cluster betreibt das Information Security Network Oberösterreich. Es ist als Tor zu Anbietern von Dienstleistungen sowie Beratern im Bereich Informationssicherheit und als Orientierungshilfe konzipiert. Es bringt somit Anbieter und Berater mit Firmen, die dieses Angebot nutzen wollen, zusammen. Es gibt Leistungen und Angebote zur Sensibilisierung und Unterstützung von oö. Unternehmen sowie Know-how-Transfer durch Kooperationsprojekte", erläutert Landesrat Achleitner.

Das Information Security Network Oberösterreich umfasst aktuell 37 Unternehmen, Forschungseinrichtungen, Bildungseinrichtungen und andere Organisationen. Einige Beispiele für die Angebote des IT-Clusters bzw. des Information Security Network Oberösterreich:

- Hack'aware – KMU-Security Quickcheck**:** Hackerangriffe sind eine Gefahr für alle Branchen und betreffen längst nicht mehr nur die Big Player, sondern immer mehr auch kleine und mittlere Unternehmen haben oft nicht die nötigen Mittel und die Manpower, um sich umfassend zu schützen. Mit dem KMU Security Quickcheck hat der IT-Cluster ein Tool entwickelt, das einen schnellen Überblick über den Status der IT-Sicherheit in Unternehmen verschafft. Es handelt sich dabei um eine Orientierungshilfe, die als Grundlage für weiterführende Gespräche mit internen oder externen Cybersecurity-Profis dient.
- AI & IT-Security Landscape: Eine digitale Landkarte verrät jetzt auf den ersten Blick, welche oberösterreichischen Unternehmen in den Bereichen Künstliche Intelligenz und IT-Security tätig sind und höchste Qualitätsstandards erfüllen. Die Landscape dient als Kompass, ermöglicht rasche Orientierung und soll den Standort OÖ als IT-Region pushen. Die AI & IT-Security Landscape OÖ wurde erstmals auf der jährlichen Fachveranstaltung SHFT im September 2022 präsentiert. Sie ist auch ein Vernetzungstool für potenzielle Kooperationspartner. Aus Sicht der Experten wird die Bedrohungslage in der digitalen Welt immer subtiler und gefinkelter. Angreifer entwickeln ihre Taktiken ständig weiter, sodass der Einsatz von Technologien für Künstliche Intelligenz (KI) und Maschinelles Lernen (ML) nicht mehr wegzudenken ist. Der Trend, der sich immer mehr verstärkt, ist ein zweischneidiger. KI und Machine

Learning wird in beiden Richtungen genutzt: Von Cyberkriminellen, um die Angriffe noch raffinierter und schneller zu entwickeln, und in der Cyber Security, um die Sicherheit zu erhöhen und schneller und automatisierter auf Angriffe reagieren zu können.

- Schulungsangebot „TAHITI“: 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 oö. Standortagentur Business Upper Austria und oberösterreichischen Unternehmen ein umfangreiches Weiterbildungsformat entwickelt, das optimal auf die Bedürfnisse der Betriebe abgestimmt wurde.
- Erfahrungsaustauschrunde Informationssicherheit: In dieser Gruppe treffen regelmäßig IT-Verantwortliche/-Mitarbeiter mit Bezug zu Informationssicherheit und/oder Datenschutz, CISOs, Risikomanager, Datenschutzbeauftragte, Verantwortliche aus dem Umfeld IT-Infrastruktur, Intern tätige Security Engineers aus dem Unternehmensumfeld sowie Informationssicherheit-Dienstleister und Experten zum Austausch über Informationssicherheit und Datenschutz. Organisiert wird die Erfahrungsaustauschrunde vom IT-Cluster und dem Softwarepark Hagenberg.

Förderungen für Maßnahmen zur Verhinderung und Abwehr von Cyber-Crime:

- Im Rahmen der Initiative „Digitalregion Oberösterreich“ gibt es eine Förderung, die sich an kleine und mittlere Unternehmen mit einer oberösterreichischen Betriebsstätte richten, die Mitglied der Wirtschaftskammer OÖ und des Qualifizierungsverbundes Digitale Kompetenz & IT-Security sind. Förderbar sind Investitionen in Hardware/Software samt Implementierungsdienstleistungen und IT-Security-Maßnahmen technischer und/oder organisatorischer Art, die nachweislich der Weiterentwicklung, Einführung oder Verbesserung der IT-Security im Unternehmen dienen. Die Förderhöhe beträgt 25 Prozent der nachgewiesenen Kosten bzw. max. 10.000 Euro.
- Weiters gibt es gemeinsame Unterstützungsmaßnahmen von Land OÖ und Wirtschaftskammer OÖ, beispielsweise durch einen zusätzlichen Bonus für IT-Sicherheitsmaßnahmen im Rahmen des erfolgreichen Programms „Digital Starter“.

Daten & Fakten zum Thema „Cyber-Crime“:

- Laut Statistik Austria verfügen **90 % der heimischen Haushalte über einen Internet-Zugang**. Mehr als 80 Prozent der Bürger in allen Altersschichten geben an, über e-Mailverkehr zu kommunizieren. Knapp 60 Prozent der Bevölkerung tätigen zum Beispiel auch Einkäufe über Online-Plattformen.
- In der aktuellen Studie der EU-Kommission zum **Digitalisierungsgrad** in den 27 Mitgliedsländern ist **Österreich** im Vorjahr vom 13. Platz **auf den 10. Platz nach vorne gerückt**.
- Platz 10 nimmt Österreich auch in der Kategorie „Integration digitaler Technologien“ im Wirtschaftsleben ein. Verantwortlich für diese gute Performance sind herausragende Werte bei der digitalen Durchdringung der KMU, bei der Anwendung des digitalen Info-Austauschs sowie beim Einsatz sozialer Medien.

Die Daten unterstreichen: **Oberösterreich ist mit Haushalten und Betrieben längst etablierter Teil der digitalen Welt – und damit auch der kriminellen Energie dort tätiger Akteure ausgesetzt**. Wir hoch diese kriminelle Energie ist, zeigen die neuesten Daten des Bundeskriminalamtes:

<u>Kleinstrukturierte und großangelegte Internet-Kriminalität in Österreich</u>:

Das Bundeskriminalamt unterscheidet in seiner Deliktsauflistung für 2021 zwei Tatmodelle:

1) „Cybercrime im engeren Sinn“: Dabei sind Netzwerke der Informations- und Kommunikations-Technologie das Angriffsziel
2) „Cybercrime im weiteren Sinn“: Dabei sind Netzwerke der Informations- und Kommunikations-Technologie das Tatwerkzeug, um Nutzern oder Betrieben Schaden zuzufügen.

<u>Cybercrime insgesamt in Österreich 2021</u>:

Cybercrime im 5-Jahresvergleich			
Jahr	Anzahl der angezeigten Straftaten	Anzahl der geklärten Straftaten	Aufklärungsquote (gerundet)
2017	16.804	6.470	38,5 %
2018	19.627	7.332	37,4 %
2019	28.439	10.192	35,8 %
2020	35.915	12.012	33,4 %
2021	46.179	17.020	36,9 %

Veränderung der Aufklärungsquote in %-Punkten im Vergleich zum Vorjahr			
	Jahr 2020 33,4 %	Jahr 2021 36,9%	+3,4 %-Punkte

Tabelle 2:
Entwicklung der Anzeigen, geklärten Fälle und der Aufklärungsquote von Cybercrime 2017 bis 2021 (Fünf-Jahres-Vergleich)

Cyberkriminalität im engeren Sinn: Gezielte Attacken auf Netzwerke und Daten:

Delikt	Angezeigte Fälle 2020	Angezeigte Fälle 2021	Geklärte Straftaten 2020	Geklärte Straftaten 2021
§ 107c StGB	329	395	253	299
§ 118a StGB	816	952	113	165
§ 119 StGB	12	14	5	11
§ 119a StGB	67	58	12	4
§ 126a StGB	361	354	78	64
§ 126b StGB	71	95	10	12
§ 126c StGB	354	540	66	46
§ 148a StGB	10603	12 701	1723	2182
§ 225a StGB	301	375	199	112
Gesamt	12914	15484	2459	2895

Tabelle 3:
Angezeigte Fälle und geklärte Straftaten von Cybercrime im engeren Sinn nach Paragrafen des StGB 2021 im Vergleich zu 2020.

§ 107c StGB (Fortdauernde Belästigung im Wege der Telekommunikation oder eines Computersystems)
§ 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)
§ 119 StGB (Verletzung des Telekommunikationsgeheimnisses)
§ 119a StGB (Missbräuchliches Abfangen von Daten)
§ 126a StGB (Datenbeschädigung)
§ 126b StGB (Störung der Funktionsfähigkeit eines Computersystems)
§ 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten)
§ 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch)
§ 225a StGB (Datenfälschung)

„Cybercrime im engeren Sinn“ = gezielte Attacken auf private, betrieblich oder öffentliche Netzwerke der Informations- und Kommunikationstechnologie.

Internet-Kriminalität im weiteren Sinn: IKT-Anlagen als „Tatwerkzeug“

Tabelle 4: Jahresvergleich 2020 und 2021: Angezeigte Fälle von Cybercrime im weiteren Sinn nach Paragrafen

Delikt	Angezeigte Fälle 2020	Angezeigte Fälle 2021	Geklärte Straftaten 2020	Geklärte Straftaten 2021
Internetbetrug				
§ 146 StGB	16.279	19.224	5.639	7.138
§ 147 StGB	1.761	2.246	580	701
§ 148 StGB	740	970	407	509
Internetbetrug-Gesamt	**18.780**	**22.440**	**6.626**	**8.348**
Sonstige Kriminalität im Internet				
§ 105 StGB	0	47	0	30
§ 106 StGB	0	23	0	17
§ 107 StGB	0	1.303	0	1.124
§ 107a StGB	1	459	1	423
§ 115 StGB	0	88	0	80
§ 144 StGB	778	1.639	83	111
§ 145 StGB	72	165	13	20
§ 207a StGB	1.702	1.921	1.528	1.775
§ 207b StGB	22	9	21	9
§ 208a StGB	142	121	102	87
§ 218 StGB	7	18	4	12
§ 223 StGB	45	87	30	60
§ 224 StGB	23	25	16	19
§ 228 StGB	1	0	1	0
§ 229 StGB	1	0	0	0
§ 231 StGB	38	37	15	19
§ 232 StGB	13	16	10	10
§ 241a StGB	1	1	1	0
§ 283 StGB	2	262	2	246
§ 27 SMG	1.154	1.201	905	941
§ 28 SMG	9	15	8	15
§ 28a SMG	63	45	58	40
§ 30 SMG	29	31	26	29
§ 31 SMG	0	1	0	1
§ 31a SMG	0	1	0	1
§ 3a VerbotsG	0	3	0	2
§ 3d VerbotsG	0	2	0	2
§ 3g VerbotsG	118	651	103	624
§ 3h VerbotsG	0	84	0	80
Sonstige Kriminalität im Internet gesamt	**4.221**	**8.255**	**2.927**	**5.777**
Internetkrimi-nalität gesamt	**35.915**	**46.179**	**12.012**	**17.020**

Kernergebnisse Studie „Cyber Security in Österreich 2022“ (KPMG und „Kompetenzzentrum Sicheres Österreich“):