KSÖ T Kompetenzzentrum Sicheres Österreich

SICHER.TIROL



E-Scooter-Tour begeistert Volksschüler

Foto: LPD Tirol

Sicherer Schulweg

Die TIROLER und der Verein „Sicheres Tirol“ setzen auf Prävention: In einer Kooperation vermitteln sie Schulkindern Sicherheitswissen im Straßenverkehr. **Seite 6**

Mobiler Escape-Room

Mit dem europaweit einzigartigen fahrbaren Escape-Room bringt die Tiroler Polizei spannende Rätsel rund um Sicherheitsfragen zu den Bürgern. **Seite 11**

Betrügerische Invests

KI-generierte Fake-Videos mit Prominenten verleiten immer wieder zu betrügerischen Investments. Warum der Betrag von 250 Euro ein Warnsignal ist. **Seite 13**

SONDERBEILAGE DER Tiroler Tageszeitung



Jeder achte Cyberangriff in Österreich war im vergangenen Jahr erfolgreich. Fast jeder dritte legte ein Unternehmen länger lahm. Foto: iStock

Updates, Virenschutz, Firewall – und trotzdem gehackt?

Beim IT-Security Roundtable von KSÖ Tirol und Strong-IT trafen sich rund 250 IT-Verantwortliche großer Betriebe und Einrichtungen. Was dort Thema war, gilt auch für jeden Haushalt.

Von David Winkler

Am 24. September saßen im Congress Innsbruck Polizei, BKA, LKA, Wirtschaft und Sicherheitsfachleute in einem Raum. Den „IT-Security Roundtable“ hat Strong-IT vor über zehn Jahren als kleine Runde gegründet, heuer fand er erstmals gemeinsam mit dem KSÖ Tirol statt. Landespolizeidirektor Helmut Tomac brachte es auf den Punkt: „Cybercrime ist kein Randphänomen mehr, sondern ein strategisch organisiertes Geschäftsmodell.“

Ich breche seit 25 Jahren in Computersysteme ein, seit 2004 beruflich und im Auftrag von Unternehmen. Hineingekommen und bis zu den Kronjuwelen vorgedrungen bin ich bis heute in über 90 % der Aufträge. Selten, weil eine Firewall oder Antivirus gefehlt hätte.

Hohe Erfolgsquote

Robert Lamprecht (KPMG) bestätigte an diesem Abend: Jeder achte Cyberangriff in Österreich war im vergangenen Jahr erfolgreich, fast jeder dritte legte ein Unternehmen länger lahm.

Wie kann das sein, trotz Updates und Virenschutz? Ein Autopilot hält bei ruhigem Wetter zuverlässig den Kurs. Im Sturm braucht es wache Piloten, eine gewartete Maschine und Training im Simulator. Updates, Virenschutz und Firewall sind so ein Autopilot, im Betrieb wie im Wohnzimmer.



Foto: Strong IT GmbH

„Seit 25 Jahren breche ich in Computersysteme ein – immer legal, seit 2004 beruflich.“

David Winkler, Gründer und Geschäftsführer der Strong-IT GmbH in Innsbruck

Angreifer melden sich an

Angreifer fliegen einfach daran vorbei. Sie brechen nicht ein, sie melden sich an: mit Zugangsdaten aus einem Datenleck oder über die E-Mail eines gehackten Lieferanten. Dann bewegen sie sich im Firmennetz wie ein Mitarbeiter, schalten Schutzprogramme und Datensicherungen ab und arbeiten sich zu den wichtigsten Daten vor. Brigadier Martin Grasel vom Bundeskriminalamt beschrieb genau diesen Ablauf. Oft gibt es keinen oder viel zu spät Alarm, selbst bei Rund-um-die-Uhr-Überwachung, denn für den Autopiloten sieht alles normal aus.

Zu Hause läuft es gleich. Im September rief bei einer Tirolerin eine angebliche Bankmitarbeiterin an, um verdächtige Abbuchungen zu stoppen. Das Opfer bestätigte dafür mehrere Freigaben in der Banking-App und gab so Überweisungen an Betrüger frei. Der Schaden: fünfstellig. Die App wurde nicht geknackt, die Tür wurde sozusagen von innen geöffnet.

Wird bei Ihnen eingebrochen, sichert die Polizei die Spuren und sucht die Täter. Das neue Schloss bauen Sie mit dem Fachbetrieb ein.

Die Polizei ermittelt

Bei Cyberangriffen ist es genau so: Die Polizei ermittelt und konzentriert sich auf Fälle mit großem Schaden und organisierte Tätergruppen. Über internationale Zusammenarbeit warnt sie jedes Jahr mehr als 50 österreichische Firmen, bevor deren Daten verschlüsselt werden. Jede Anzeige hilft, Serien zu erkennen. Wurde Geld überwiesen: sofort die Bank anrufen, dann zur Polizei. Betriebe erreichen rund um die Uhr die Cyber-Security-Hotline der Wirtschaftskammer unter 0800 888 133.

Am Roundtable zeigte Matteo Longo (Strong-IT) live, wie Angreifer vorgehen, Martin Plattner (Axians), warum Industrieanlagen eigene Regeln brauchen, Michael Lackner (Strong-IT) und Philip Scheidl (CrowdStrike), wie man Angriffe früh erkennt. Die gemeinsame Botschaft: Sicherheit ist kein einmaliges Produkt, sondern ständiges Besserwerden. Das gilt für Konzerne wie für Familien.

„Angreifer brechen nicht ein, sie melden sich an – mit Zugangsdaten aus einem Datenleck.“

David Winkler, Gründer und GF der Strong-IT GmbH, Innsbruck

Was jeder tun kann

Gehen Sie davon aus, dass ein Passwort von Ihnen schon im Netz liegt.

Zuerst das Mail-Konto schützen: Wer es übernimmt, kommt über „Passwort vergessen“ in alle anderen Konten. Zwei-Faktor-Anmeldung einschalten, auch bei Bank- und Handy-Konto.

Für jeden Dienst ein eigenes Passwort, verwaltet von einem Passwortmanager.

Keine seriöse Bank ruft an und verlangt eine Freigabe. Auflegen und selbst über die Nummer auf der Bankkarte zurückrufen.

Push-Nachricht für jede Buchung einschalten und ein niedrigeres Überweisungslimit festlegen.

Ein Familien-Codewort gegen Schockanrufe und nachgemachte Stimmen ausmachen.

Automatische Updates bei Handy, PC und Router einschalten. Alle Altgeräte ohne Updates gehören ausgetauscht.



Das Präsidium des KSÖ Tirol mit Helmut Tomac (l.), Isolde Stieg (TIROLER Versicherung, 2. v. l.), Silvia Lieb (2. v. r.) und Franz Mair (TIROLER Versicherung; r.) mit CEO Strong IT David Winkler (Mitte). Foto: LPD

TIPP

Datendiebstahl: Wenn Cyber-Kriminelle zuschlagen

Immer häufiger werden Unternehmen Opfer von Cyberangriffen. Dabei geht es den Tätern nicht nur darum, Computersysteme lahmzulegen, sondern auch um den Diebstahl sensibler Daten. Die Folgen können sowohl Firmen als auch Privatpersonen treffen.

Wie funktionieren solche Angriffe? Kriminelle verschaffen sich beispielsweise über gefälschte E-Mails, gestohlene Passwörter oder Sicherheitslücken Zugang zu Firmennetzwerken. Dort stehlen sie Daten und verschlüsseln häufig wichtige Systeme, um den Betrieb lahmzulegen. Anschließend fordern sie Lösegeld. Sie drohen damit, gestohlene Informationen zu veröffentlichen, wenn nicht bezahlt wird.

Welche Daten sind betroffen? Gestohlen werden etwa personenbezogene Daten von Personal und Kunden, Ausweiskopien, Zugangsdaten oder sensible Firmendaten.

Was können Unternehmen tun? Wichtig sind regelmäßige Sicherheitsupdates, sichere Passwörter, Mehrfach-Authentifizierung und getrennt aufbewahrte Datensicherungen sowie Awareness-Schulungen für Mitarbeiter. Nach einem Angriff sollten Firmen rasch IT-Fachleute einschalten, Beweise sichern, Anzeige erstatten und mögliche Meldepflichten prüfen. Die Polizei veröffentlicht solche Fälle nicht und führt auch keine Sicherstellungen von Firmen-IT durch, sondern unterstützt ausschließlich bei der Sicherung der Beweismittel und ist beratend tätig.

Was bedeutet das für Privatpersonen? Gestohlene Daten können für Betrugsversuche missbraucht werden. Kriminelle versuchen etwa, E-Mail- oder Social-Media-Konten zu übernehmen oder mit fremden persönlichen Daten neue Konten zu eröffnen. Auch täuschend echte Nachrichten, beispielsweise zu einer angeblich offenen Hotelbuchung oder eines angeblich dringenden Check-in-Vorganges, sind möglich. Deshalb gilt: keine unbekannten Links öffnen, Zahlungsaufforderungen über offizielle Kontaktwege prüfen und für jedes Konto ein eigenes, sicheres Passwort verwenden sowie Mehrfach-Authentifizierung aktivieren. Sind Zugangsdaten betroffen, müssen Passwörter sofort geändert und verdächtige Kontoaktivitäten kontrolliert werden.

Weitere Hilfe im Internet: Die österreichische Plattform *watchlist-internet.at* informiert über aktuelle Betrugsmaschen. Weitere Tipps bieten *nomoreransom.org* und *phishen-impossible.at*



Foto: BMI

Martin Grasl, Ermittlungsleiter des Cybercrime Competence Center im Bundeskriminalamt

Martin.Grasl@bmi.gv.at

Sicherheit im Fokus: Tiroler E-Scooter-Tour begeistert Volksschulkinder

Die Tiroler Polizei schulte für das Land Tirol auf Initiative des KSÖ über 2.100 Kinder im Umgang mit E-Scootern in einer Bezirkstour für Volksschulkinder.

Übung macht den Meister" – unter diesem Motto wurde eine landesweite Initiative gestartet, die nicht nur in Tirol, sondern in ganz Österreich für Aufsehen gesorgt hat. Für die besonderen Leistungen in der Sicherheitsprävention belegte das Projekt den hervorragenden 2. Platz auf österreichweiter Ebene.



Auch Verkehrslandesrat René Zumtobel besuchte die Veranstaltung und zeigte sich beeindruckt vom Wissen der Kinder zum Thema E-Scooter. Fotos: LPD/Stefan Eder

Mehr als 100 Schulklassen

Die Tiroler Polizei führte über die Initiative des Kompetenzzentrums Sicheres Österreich (KSÖ), Landesklub Tirol, eine umfassende Tour durch das Land durch. Von der Frühjahrsmesse in Innsbruck über Imst, Prutz, Pfunds und Kematen bis hin zum feierlichen Abschluss beim SZentrum in Schwaz wurden mehr als 100 Schulklassen mit insgesamt über 2.100 Kindern der 3. und 4. Volksschulklasse erreicht.

Im Zentrum standen praxisnahe Schulungen, um den Kindern den sicheren Umgang mit E-Scootern zu vermitteln. In speziellen Parcours lernten die Schülerinnen und Schüler:

- Die korrekte Lenk- und Bremstechnik.
- Die geltenden Verkehrsregeln und die erlaubten Fahrbereiche.
- Die Bedeutung des Helms und die Regeln für die Teilnahme am Straßenverkehr.
- Die Gefahren im Umgang mit E-Scootern, um Unfälle zu vermeiden.



Gruppeninspektor Erwin Vögele moderierte die Veranstaltung am Vorplatz des SZentrums in Schwaz.



In speziellen Parcours lernten Kinder aus ganz Tirol – hier auf dem Bild aus dem Bezirk Schwaz – den sicheren Umgang mit E-Scootern.

Die Notwendigkeit dieser Prävention unterstreicht Landespolizeidirektor und KSÖ-Präsident Helmut Tomac: Da E-Scooter und E-Bikes immer mehr das Straßenbild prägen, steigen auch die Unfallzahlen. Durch die Kombination aus Schulungen und gezielten Schwerpunktkontrollen möchte das KSÖ gemeinsam mit dem Land Tirol und der Polizei das Unfallrisiko nachhaltig senken.

Projektleiter Erwin Vögele von der Landespolizeidirektion Tirol betont zudem, dass die E-Scooter-Schulungen fest in die jährliche Verkehrserziehung integriert sind. Unterstützt wurde das Vorhaben durch den Verkehrssicherheitsfonds Tirol, der E-Scooter finanzierte, welche nun auch bei den praktischen Übungen eingesetzt werden.

Verkehrslandesrat René Zumtobel hob im Schwerpunkt des Landes hervor, dass die Zielgruppen direkt erreicht werden müssen. Da E-Scooter für viele Kinder heute eine ebenso wichtige Rolle spielen wie früher das Fahrrad, ist die Einbindung in die offizielle Verkehrserziehung der Schlüssel für eine sichere Mobilität in ganz Tirol.





Mit Sujets macht das Land Tirol in der Kampagne „Gemeinsam & fair im Straßenverkehr" auf Regeln für E-Scooter aufmerksam.



Über 500 Kinder aus dem Bezirk Schwaz nahmen an der Veranstaltung teil.

Regeln für E-Scooter

Technik: Blinker an beiden Lenkerenden, Klingel/Hupe, mind. eine Bremse, Rückstrahler (weiß, rot, gelb) sowie Beleuchtung (weiß vorne, rot hinten) sind Pflicht. Max. 25 km/h und 600 Watt.

Fahrregeln: Radwegnutzung obligatorisch, sonst Fahrbahn; Gehsteig verboten. Nur Einzelperson erlaubt; Gütertransport nur in festen Behältnissen/Rollertaschen (Lenkertaschen verboten).

Sicherheit: Alkoholgrenze 0,5 Promille. Helmpflicht für Personen unter 16 Jahren.



Superhelden unter sich: Super-Mike und Tiroli haben sich zusammengetan, um Kindern wertvolles Sicherheitswissen zu vermitteln. Fotos: TIROLER

Jeder Unfall ist einer zu viel: Gemeinsam für sichere (Schul-)Wege

Die TIROLER VERSICHERUNG und der Verein Sicheres Tirol setzen auf Prävention von Anfang an – vor allem für Schulkinder, die erstmals allein im Straßenverkehr unterwegs sind.

Sie sind ein ungleiches Paar: der eine kugelrund und quietschgrün, stets mit frechem Käppi unterwegs, der andere ein echter Superheld mit Flügeln und verwegener Maske. Doch Tiroli und Super-Mike haben einen gemeinsamen Auftrag: Kindern auf spielerische Weise zu zeigen, worauf es im Alltag, beim Sport und im Straßenverkehr ankommt, damit sie sicher unterwegs sind.

Für viele Kinder ist der Schulweg die erste Gelegenheit, sich allein im Straßenverkehr zu bewegen. Während die Kleinen ihre neue Freiheit genießen, haben viele Eltern beim täglichen Weg zur Schule gemischte Gefühle. Denn Kinder können Gefahren im Straßenverkehr oft noch nicht richtig einschätzen und sind deshalb besonders schutzbedürftig. Genau hier kommen Tiroli und Super-Mike und deren „Paten" ins Spiel: die TIROLER und der Verein Sicheres Tirol. Gemeinsam verfolgen sie das Ziel, Unfälle zu verhindern, bevor sie passieren, und das Sicherheitsbewusstsein bereits bei den Jüngsten zu stärken. „Die Sicherheit von Kindern hat für uns oberste Priorität. Prävention ist ein zentraler Teil unseres Auftrags, denn jeder Unfall mit einem Kind ist einer zu viel", erklärt Vorstandsdirektorin Isolde Stieg die Ursprünge der Kooperation zwischen TIROLER und Verein Sicheres Tirol.

Für Peter Hölzl, Vizepräsident des Vereins Sicheres Tirol, ist genau dieses gemeinsame Engagement der Schlüssel zum Erfolg: „Nur wenn öffentliche Einrichtungen, Unternehmen und engagierte Organisationen zusammenarbeiten, kann Sicherheit nachhaltig verbessert werden!", stellt er fest.

Mach dich sichtbar!

Die Maßnahmen sind vielfältig: Bereits seit acht Jahren versorgen die TIROLER und der Verein Sicheres Tirol die Erstklässler:innen mit Schulstartpaketen: Rund 9.000 Kinder erhalten jedes Jahr eine Sicherheitsweste, einen reflektierenden Anhänger für die Schultasche sowie Informationsunterlagen für Kinder und Eltern. Ziel ist es, die Sichtbarkeit zu erhöhen und bereits die Jüngsten für Gefahren im Straßenverkehr zu sensibilisieren.

Gemeinsam mit dem Kuratorium für Verkehrssicherheit (KfV) setzen die Partner aber auch auf sichtbare Zeichen im Straßenraum. Im Rahmen der Initiative „Achtung Kinder!" wurden bereits mehr als 600 Hinweistafeln an Tiroler Gemeinden verteilt. Sie erinnern Autofahrerinnen und Autofahrer daran, in Bereichen, wo viele Kinder unterwegs sind, besonders vorsichtig und aufmerksam zu fahren.

Ergänzt werden diese Maßnahmen durch die landesweite Aktion „Mach dich sichtbar!". Dabei weisen Banner auf die Bedeutung von Sichtbarkeit im Straßenverkehr hin. Diese Initiative wurde gemeinsam vom Verein Sicheres Tirol, TIROLER, Land Tirol, Landespolizeidirektion Tirol und dem Kuratorium für Verkehrssicherheit umgesetzt.

Die Bedeutung solcher Präventionsmaßnahmen zeigt sich insbesondere in den Herbst- und Wintermonaten. Kürzere Tage, Nebel und schlechte Sichtverhältnisse erhöhen das Unfallrisiko deutlich. Gerade deshalb sind Sichtbarkeit und Aufmerksamkeit entscheidende Faktoren für einen sicheren Schulweg. Super-Mike und Tiroli sind deswegen auch in Zukunft gemeinsam unterwegs – für ein Stück mehr Sicherheit für unsere Kleinsten.



Foto: TIROLER/Simon Rainer

„Große Herausforderungen lassen sich nur gemeinsam bewältigen. Deshalb engagieren wir uns mit dem Verein Sicheres Tirol für mehr Sicherheit und Prävention im Alltag."

Franz Mair, Vorstandsvorsitzender TIROLER



Foto: TIROLER/Simon Rainer

„Prävention ist ein zentraler Teil unseres Auftrags. Jeder Unfall mit einem Kind ist einer zu viel."

Isolde Stieg, Vorstandsdirektorin TIROLER



Kleine Maßnahmen, große Wirkung: Warnwesten und Reflektoren an der Schultasche erhöhen die Sichtbarkeit im Straßenverkehr.



Achtung Kinder! Mit Armin Singer (Ressortleiter Vertrieb, TIROLER), Arno Thrainer, (Bereichsleiter Fachbereich Key Account, TIROLER), Peter Hölzl (Vizepräsident Verein Sicheres Tirol), Manfred Gutwenger (Bereichsleiter Fachbereich Key Account, TIROLER), Markus Baumann (Bürgermeister Gemeinde Ranggen), Valentina Sassmann (Amtsleiterin Marktgemeinde Fulpmes), Gerhard Meister (Geschäftsführer Verein Sicheres Tirol), Marco Mösl (Bürgermeister Gemeinde Natters).

Tipps für einen sicheren Schulweg

- Reflektierende Elemente an Schultasche, Jacke oder Schuhen anbringen.
- Helle, gut sichtbare Kleidung tragen, besonders in der dunklen Jahreszeit.
- Den Schulweg mehrmals gemeinsam üben und auf potenzielle Gefahrenstellen hinweisen.
- Alternativrouten kennen, falls Baustellen oder Sperren den gewohnten Weg verändern.
- Ausreichend Zeit einplanen, damit Kinder nicht unter Stress unterwegs sind.
- Straßen ausschließlich an sicheren und gut übersichtlichen Stellen überqueren.
- Blickkontakt mit Autofahrerinnen und Autofahrern suchen, bevor die Straße betreten wird.
- Der sicherste Schulweg ist nicht immer der kürzeste. Nehmen Sie lieber einen etwas längeren Weg in Kauf, wenn dafür sichere Gehwege, Zebrastreifen oder Ampeln genutzt werden können.
- Eltern sollten Vorbilder sein und Verkehrsregeln konsequent einhalten.
- Sichtbarkeit rettet Leben: Reflektierende Kleidung kann die Erkennbarkeit bei Dunkelheit deutlich verbessern.



Zuerst wird in einem Chat Vertrauen aufgebaut, es entsteht eine Freundschaft, in der die Jugendliche unter Druck gesetzt wird. Fotos: iStock

Neue Gefahr aus dem digitalen Raum: „The COM“ – erst Freundschaft, dann Druck

Unter Druck gesetzt, bedroht, zu schweren Straftaten genötigt. Das ist eine neue Gefahr, die Jugendlichen in Chats droht. Wie Eltern diese Bedrohung ihrer Kinder erkennen können, erklären Experten.

Jugendliche suchen Orientierung, Gemeinschaft und Anerkennung zunehmend online. Gaming, soziale Medien und Chats sind soziale Lebensräume. Ein digitaler Raum kann sich sicher anfühlen – und gezielt genutzt werden, um Vertrauen aufzubauen und auszunutzen. Psychisch vorbelastete, ausgegrenzte, sozial isolierte Kinder und Jugendliche gelten für solch einen Vertrauensmissbrauch als besonders anfällig.

Das Phänomen „The COM“ zeigt, wie aus einem zunächst harmlosen Online-Kontakt eine gefährliche Situation entstehen kann. Bei „The COM“ handelt es sich um ein international agierendes, gewaltorientiertes Netzwerk, welches in unterschiedlichen Untergruppen und Chatforen Kinder und Jugendliche „ködert“, sie in Folge manipuliert, unter Druck setzt und zu schweren Straftaten nötigt.

Häufig beginnt alles mit Aufmerksamkeit und Anerkennung. Aus gemeinsamen Interessen entstehen Gespräche, persönliche Themen werden geteilt und der Kontakt verlagert sich in private Chats. Später werden diese Informationen für Druck, Drohungen oder Erpressung genützt. Aufmerksam sollten Eltern werden, wenn sich ein Kind deutlich und nachhaltig verändert: etwa durch sozialen Rückzug, Geheimhaltung von Handy- oder Online-Kontakten oder neue unbekannte Online-Bekanntschaften. Kommt es zu Veränderungen im Freundeskreis oder von Interessen? Zeigt das Kind starke Reaktionen nach Chats, Fixierung auf Personen oder Inhalte oder „Wir gegen die“-Denken? Beschäftigt es sich mit Gewalt oder weicht bei Fragen zu Online-Kontakten aus?

Keines dieser Anzeichen beweist für sich allein eine Radikalisierung. Entscheidend sind mehrere Veränderungen und deren Dauer. Eine vertrauensvolle Beziehung ist ein wesentlicher Schutzfaktor. Interessiertes Nachfragen hält den Kontakt aufrecht:

- Mit wem spielst du?
- Welche Apps verwendest du?
- Ist dir online schon mal etwas Unangenehmes passiert?

Vorwürfe, Verbote oder Strafen können Vertrauen zerstören. Eine wichtige Botschaft lautet: „Egal, was passiert ist – du musst damit nicht allein bleiben. Wir schauen gemeinsam, was wir tun können.“

Regeln für Apps und Spiele, Privatsphäre-Einstellungen und Gespräche über persönliche Daten und Bilder schaffen Sicherheit. Bei Drohungen, Erpressung oder massivem Druck: Ruhe bewahren, Kind unterstützen, Nachrichten sichern und Polizei verständigen. Das Kind nicht beschämen. Die Schuld liegt immer beim Täter!

Es geht nicht darum, soziale Medien, Gaming oder das Internet generell als Gefahr darzustellen. Junge Menschen sollen digitale Räume sicher und selbstbestimmt nutzen können. Dazu gehört, Online-Kontakte kritisch zu hinterfragen.

Nicht jeder Ort, der sich sicher anfühlt, ist tatsächlich sicher. Kinder im digitalen Raum zu schützen, bedeutet, aufmerksam zu bleiben, Interesse zu zeigen und Gespräche ohne Vorurteile zu ermöglichen.

Hinsehen. Nachfragen. Zuhören. Handeln, wenn es notwendig wird. Das ist digitale Prävention.

Tipps für Eltern und Erziehungsberechtigte

1. Im Gespräch bleiben und Entwicklungen ernst nehmen: Interesse an der digitalen Lebenswelt zeigen und Veränderungen wie Rückzug, Geheimhaltung, Angst, auffälliges Verhalten und Selbstverletzung ernst nehmen.
2. Kontakte und Privatsphäre schützen: Online-Kontakte kritisch hinterfragen. Persönliche Daten, Fotos und Aufenthaltsorte nicht an Unbekannte weitergeben. Forderungen nach Geheimhaltung sind ein Warnsignal.
3. Bei Druck und Drohungen richtig handeln: Ruhe bewahren, das Kind unterstützen und den Kontakt zum Verursacher nicht selbst suchen. Nachrichten, Profile und Screenshots sichern.
4. Vertrauen und Hilfe: Kinder nicht beschämen oder vorschnell bestrafen. Sie ermutigen, sich an Sie zu wenden. Bei konkreten Verdachtsfällen oder strafrechtlich relevanten Vorgängen die Polizei verständigen.
Die Polizei hört zu, nimmt die Anliegen ernst, behandelt sie mit der notwendigen Vertraulichkeit und bietet Hilfe und Unterstützung.



Eltern, die bemerken, dass das Vertrauen ihres Kindes im Web missbraucht wird, sollten folgende Botschaft vermitteln: Egal, was passiert ist, du bleibst damit nicht allein.

Sicherheit beginnt mit dem Gefühl von Zugehörigkeit

Was braucht es, damit sich Kinder und Jugendliche in ihrer Schule wirklich sicher fühlen? Eine Frage, die seit dem Amoklauf an einer Grazer Schule im Juni 2025 eine besondere gesellschaftliche Bedeutung bekommen hat.

Während mit Schulleitung und Lehrern vor allem über bauliche und organisatorische Sicherheitsmaßnahmen gesprochen wurde, wollte das Präventionsprojekt #SafeSpaceSchule eine andere, ebenso wichtige Perspektive in den Mittelpunkt stellen: Wie erleben junge Menschen Sicherheit selbst? Was gibt ihnen Halt – und was können wir alle dazu beitragen, dass Schule ein sicherer Ort bleibt?



Die TeilnehmerInnen des Projektes #SafeSpaceSchule. Foto: LPD Tirol

Gemeinsam mit der Bildungsdirektion Tirol, der Staatsanwaltschaft und dem Kuratorium Sicheres Österreich (KSÖ) – Landesclub Tirol initiierte das Landeskriminalamt Tirol das Projekt #SafeSpaceSchule und lud Schülerinnen und Schüler der 5. bis 13. Schulstufe ein, ihre ganz persönliche Vorstellung kreativ umzusetzen.

In Beiträgen in Form von Kurzvideos lieferten die Jugendlichen ihre Botschaften. Sie zeigen auf, dass ein Safe Space weit mehr ist als ein geschützter Raum. Es sind Freundschaften, Vertrauen, Respekt, gegenseitige Unterstützung und der Mut, nicht wegzuschauen. Manchmal ist es eine Person, die zuhört. Ein anderes Mal ein Mitschüler, der jemanden einbezieht. Oder schlicht das Gefühl: „Hier darf ich so sein, wie ich bin.“

Genau darin liegt die besondere Stärke des Projekts. #SafeSpaceSchule macht sichtbar, dass Sicherheit nicht erst dann beginnt, wenn etwas passiert. Sie beginnt viel früher – im täglichen Miteinander.

Damit richtet sich die Initiative nicht nur an Jugendliche, sondern auch an Eltern und Erwachsene: Wir alle prägen mit unserem Verhalten das Umfeld, in dem junge Menschen leben und lernen. Zuhören, hinschauen, Grenzen respektieren, füreinander einstehen und Ausgrenzung nicht einfach hinnehmen – das sind wesentliche Bausteine eines sicheren Umfelds.

Prävention braucht dafür engagierte Partner. Das KSÖ Tirol unterstützt #SafeSpaceSchule und trägt damit wesentlich dazu bei, dass aus einer Idee ein konkretes Projekt werden kann, das Jugendliche erreicht, ihre Perspektiven sichtbar macht und gesellschaftliche Diskussion anstößt. Gerade solche Kooperationen zwischen Polizei, Bildung, Justiz und der Bevölkerung zeigen, wie viel entstehen kann, wenn Verantwortung gemeinsam getragen wird.

Denn die vielleicht wichtigste Botschaft von #SafeSpaceSchule lautet: Sicherheit entsteht nicht nur durch Maßnahmen. Sie entsteht durch Menschen, die füreinander Verantwortung übernehmen.

Sicherheit braucht uns alle: Hauptberufliche und Freiwillige Hand in Hand

Ob Polizei, Rettung oder Feuerwehr: Tirols Sicherheit beruht auf professioneller Arbeit und freiwilligem Einsatz. LH Anton Mattle über das Tiroler Sicherheitsnetz und die Bedeutung des Ehrenamts.



Fast jede und jeder Zweite in Tirol engagiert sich ehrenamtlich. LH Anton Mattle selbst war bei der Freiwilligen Feuerwehr und der Bergrettung tätig. Für ihn hat das Ehrenamt eine große Bedeutung fürs Land und die Gesellschaft. Foto: Land Tirol/Fitsch

Herr Landeshauptmann, Tirol hat das Jahr des Ehrenamts ausgerufen. Warum?
Anton Mattle: Ehrenamt ist der soziale Kitt, der unsere Gesellschaft zusammenhält. Das, was wir in Tirol haben, ist absolut keine Selbstverständlichkeit. Kaum irgendwo auf der Welt ist der freiwillige Einsatz für die Allgemeinheit so stark wie in Tirol. Fast jede und jeder Zweite engagiert sich in unserem Land freiwillig. Das Ehrenamt trägt viele Uniformen und Trachten. Es trägt aber genauso eine Trainingsjacke, eine Kochschürze oder ganz normale Alltagskleidung. Hinter dieser Zahl stehen unzählige persönliche Geschichten und ein Miteinander, das unbezahlbar ist. Das wollen wir im Jahr des Ehrenamts sichtbar machen und ausbauen.

Im Sicherheitsbereich sind sehr viele Menschen, aber nicht nur Ehrenamtliche, im Einsatz. Welche Rolle spielen haupt- und ehrenamtliche Einsatzkräfte?
Mattle: Sicherheit ist immer eine Gemeinschaftsleistung. Die Polizistinnen und Polizisten sorgen hauptberuflich für Schutz, Ordnung und rasche Hilfe. Dazu kommen die Fachkräfte in Behörden und Leitstellen sowie die haupt- und ehrenamtlichen Kräfte unserer Einsatzorganisationen. Sie bringen unterschiedliche Aufgaben, Ausbildungen und Erfahrungen mit. Entscheidend ist, dass alle im Ernstfall eingespielt zusammenarbeiten. Niemand ersetzt die oder den anderen: Gerade diese Ergänzung macht unser Sicherheitsnetz so verlässlich – vieles wäre ohne die ehrenamtlichen Mitglieder so nicht möglich. Das Feuerwehr- oder Bergrettungswesen sind zwei gute Beispiele dafür.

Was zeichnet das „Tiroler System" besonders aus?
Mattle: Den Tirolerinnen und Tirolern ist es nicht egal, was in ihrem Land passiert. Sie schauen nicht weg, sondern helfen im Ernstfall zusammen. In einer Einsatzorganisation lernt man, dass jeder seinen Beitrag leisten muss. Man kann sich aufeinander verlassen und weiß, dass man füreinander da ist. Und ich glaube, dass genau diese Haltung Tirol auszeichnet: Nicht lange reden, sondern anpacken, wenn jemand Hilfe braucht. Rund 50.000 Menschen engagieren sich ehrenamtlich in den Tiroler Einsatzorganisationen. Gleichzeitig braucht es die hohe Professionalität von Polizei und weiteren Hauptberuflichen. Beides gehört untrennbar zusammen. Dafür gebührt allen Beteiligten großer Respekt.

Sie kennen den freiwilligen Einsatz auch aus eigener Erfahrung. Welche Erfahrungen haben Sie geprägt?
Mattle: Ich bin durch meinen Vater früh der Freiwilligen Feuerwehr beigetreten, weil er damals Kommandant war. Durch meine Begeisterung fürs Bergsteigen bin ich dann auch zur Bergrettung gekommen und war lange Zeit in der Landesleitung aktiv. Aus dieser langen Zeit habe ich viele Freundschaften und ein gutes Gespür für die Menschen mitgenommen.

Was soll vom Jahr des Ehrenamts bleiben?
Mattle: Die Initiative beruht auf vier Säulen: gute Rahmenbedingungen, Service, Anerkennung und ausreichend Nachwuchs für das Ehrenamt. Wir schaffen eine niederschwellige Rechts- und Grundberatung für Ehrenamtliche, bündeln Informationen auf einer Wissensplattform und machen das Beratungs- und Weiterbildungsangebot leichter zugänglich. Politik kann Engagement nicht verordnen. Aber Politik kann dafür sorgen, dass es gute Bedingungen gibt. Auch der Versicherungsschutz und die Nachwuchsarbeit bleiben wichtige Themen. Wir schaffen Verbesserungen für das Ehrenamt, die über 2026 hinauswirken.

Welche Botschaft möchten Sie den Menschen mitgeben, die Tirol sicherer machen?
Mattle: Ein großes „Vergelt's Gott!". Mein Dank gilt allen, die im Dienst oder in ihrer Freizeit für andere da sind – von der Polizei über die Rettungsdienste bis zu Feuerwehr und Grubenwehr. Das ist das, was Tirol ausmacht.







Mobiler Escape Room der Polizei bei der Präsentation auf der Herbstmesse in Innsbruck, die Initiatoren des Escape Rooms, Erwin Vögele und Lisa Köll von der Landespolizeidirektion Tirol, der Aufsichtsratsvorsitzende der Messe, Andreas Berger, und weitere Besucher lösen Rätsel im Escape Room. Fotos: LPD

Innovation auf Rädern: Die Tiroler Polizei präsentiert fahrbaren Escape Room

Tirol setzt neue Maßstäbe in der Prävention. Ein europaweit einzigartiger mobiler Escape Room bringt spannende Rätsel und wichtige Sicherheitsbotschaften direkt zu den Bürgern.

In der modernen Polizeiarbeit geht es längst nicht mehr nur um Repression, sondern vor allem um Prävention und Kommunikation. Mit einem innovativen Projekt, das europaweit seinesgleichen sucht, geht die Tiroler Polizei nun einen entscheidenden Schritt voran: Die Einführung eines fahrbaren Escape Rooms.

Das Konzept ist so simpel wie effektiv: Ein speziell umgebauter Raum verwandelt sich in ein begehbares Rätsellabyrinth. Die Teilnehmer werden in ein Szenario versetzt, in dem sie innerhalb eines begrenzten Zeitrahmens komplexe Rätsel lösen müssen. Auf der Innsbrucker Herbstmesse wurde das Projekt der Öffentlichkeit präsentiert und stieß auf überwältigende Resonanz: Die Zeitfenster waren an allen Messetagen rasch ausgebucht. Die Nachfrage zeigte, wie sehr interaktive Formate begeistern.

Doch hinter dem Rätselspaß steckt eine wichtige Botschaft: Die sogenannte „Crime Experience" verbindet Unterhaltung mit konkreter Präventionsarbeit. Während die Teilnehmenden logisch denken und im Team kooperieren, werden sie für aktuelle Betrugsmaschen sensibilisiert und erhalten Tipps zur Einbruchsprävention. Anstatt passiv zuzuhören, verarbeiten sie Informationen, die im realen Leben vor Gefahren schützen können.

Hinter dieser Innovation steht ein engagiertes Team. Das Projekt wurde von Erwin Vögele aus der Abteilung Öffentlichkeitsarbeit der Tiroler Polizei initiiert sowie vorangetrieben und von Polizisten aus Tirol konstruiert. Ermöglicht wurde die Umsetzung durch die finanzielle Unterstützung des KSÖ – Kompetenzzentrum Sicheres Österreich.

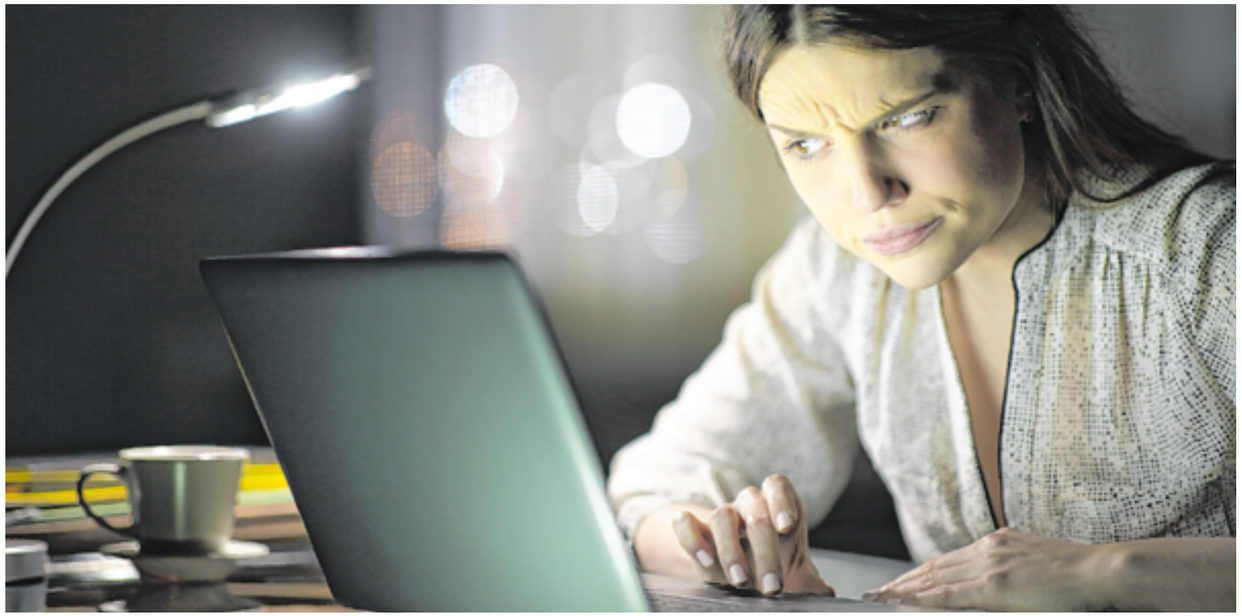
Die Mobilität des Escape Rooms ist dabei der entscheidende Vorteil. Die Polizei kann die Präventionsarbeit direkt in die Gemeinden, auf Schulhöfe oder zu Stadtfesten bringen. Damit wird die Hürde für die Bürger massiv gesenkt, in Kontakt mit den Beamten zu treten. Der fahrbare Raum dient somit als „Eisbrecher", um das Vertrauen zwischen Polizei und Bevölkerung zu stärken und einen Dialog auf Augenhöhe zu führen.



Foto: LPD

„Der neue „Escape Room" wird für Prävention, Recruiting und moderne Öffentlichkeitsarbeit eingesetzt."
Helmut Tomac, LPD und KSÖ-Tirol-Präsident

Dieses Projekt unterstreicht den Anspruch der Tiroler Polizei, innovativ zu agieren. Durch die Verbindung von Unterhaltung und Bildung wird ein Lerneffekt erzielt, der weit über den Moment des Spiels hinausgeht. Mit diesem Schritt positioniert sich Tirol als Vorreiter in Europa: Denn moderne Polizeiarbeit muss dort stattfinden, wo die Menschen sind.



Wenn per Mail oder Telefonanruf Zugangsdaten angefordert werden, dann sind größte Skepsis und Argwohn angebracht. Es handelt sich um einen Phishing-Versuch. Foto: iStock

Fallen, Fakes und fiese Tricks! Ein Überblick über einige aktuelle Betrugsmaschen

Betrug gibt es, seit es Menschen gibt. Früher meist im persönlichen Kontakt zwischen zwei Personen – heute meist übers Internet. Einige aktuelle Betrugsformen im Netz im Überblick.

Von Helmuth Lichtmannegger

Phishing. Das Herauslocken von geheimen Zugangsdaten ist nach wie vor eine der wichtigsten Betrugsmaschen. Die angeblich bald ablaufende ID-Austria verlängern, den Klimabonus beantragen (gibt's gar nicht mehr) oder eine scheinbare Rückzahlung (ÖGK/Finanzamt) erhalten – so wird versucht, an Zugangsdaten zu gelangen. Wer keine ID-Austria hat, erkennt sofort, dass es Fake ist. Wer schon, soll Kontakt mit der ID-Servicestelle zur Klärung aufnehmen. Immer: Nummer im Netz suchen und dort anfragen, woher eine Nachricht (angeblich) kommt.

Zweierlei Betrug mit booking.com. Auch mit angeblichen Rückzahlungen von Booking werden Reisende in die Phishing-Falle gelockt. Betrüger versuchen so, an die Bankdaten zu gelangen. Die Kontakt- und Reisedaten stammen dabei aus Datenlecks entweder bei der Buchungsplattform oder von einem Hotel, dessen EDV gehackt wurde. Eine fiese zweite Betrugsvariante: Scheinbar schreibt das Hotel, in dem gebucht wurde, es gäbe Probleme mit der Kreditkarte und die Daten müssten nochmals übermittelt sowie Zahlungen freigegeben werden. Finger weg: immer Hotel direkt kontaktieren.

Der Fake-Anruf der „Bankmitarbeiterin". Sobald Bankdaten in kriminelle Hände geraten sind, beginnt die Betrugsmaschinerie mit Anrufen von angeblichen Bankmitarbeitern. Da Kriminellen ja zuvor schon ins Online-Banking einsteigen konnten, verfügen sie über beeindruckendes Wissen über das Konto oder die eigene Bankberaterin. Das schafft Vertrauen, bevor, oft nach angeblich kürzlich erfolgter Überweisung ins Ausland, gefragt wird. Für die schnelle Rückholung verlangen die Täter dann TAN, TAC oder eine Freigabe in der Banking-APP. In Panik passiert das leider oft. Im Zweifel: Gespräch beenden und eigene Bank anrufen.

Fake-Rechnungen und Mahnungen. Tagtäglich passieren Hacking-Angriffe auf Netzwerke von Firmen und Institutionen. Datenlecks und der illegale Handel im „Darknet" verschaffen Kriminellen Zugang zu Informationen über Kontakt- und Kaufverhaltensdaten. Mit diesen Daten werden immer wieder und tausendfach Fake-Rechnungen oder auch Inkassomahnungen an wirklich existierende E-Mail-Accounts und Postadressen versandt. Es gilt: Wurde kein rechtswirksamer Vertrag geschlossen (auch im Internet durch Anklicken eines Zahlungsbuttons und Vorliegen von weiteren Kriterien möglich), gibt es keine Forderung.

Tipps

Niemand schenkt im Internet was her – Gratis-Versprechen niemals glauben! Geiz ist geil, wenn es um persönliche Daten geht: Immer dann, wenn Daten eingegeben oder irgendwas heruntergeladen werden soll, oder wenn irgendetwas anders ist als sonst – Finger weg von der Tastatur. Nachdenken und einfach mal nichts machen. Die Konsumentenschutz-Hotline der AK Tirol ist bei Unklarheiten und Fragen unter der kostenlosen Telefonnummer 0800/225522-1818 erreichbar.

Wenn Armin Wolf mit Herbert Kickl und Van der Bellen über „Investments" streitet

KI-generierte Fake-Videos mit prominenten TV-Moderatoren oder Politikern verleiten immer wieder zu betrügerischen Investments. Warum der Betrag von 250 Euro ein Warnsignal ist.

Von Helmuth Lichtmannegger

Oft sind es sogar bekannte und grundsätzlich vertrauenswürdige Internetseiten, auf welchen Werbeanzeigen platziert sind, die über einen Link zu angeblichen Streitgesprächen in einem TV-Studio führen. Allerdings haben diese Gespräche nie stattgefunden. Es handelt sich dabei regelmäßig um Fake-Videos. Echte Fernsehaufzeichnungen wurden dabei mit Hilfe von Programmen, getrieben von „Künstlicher Intelligenz", in Bild und Ton manipuliert und verändert. Heraus kommen schließlich Unterhaltungen rund um angeblich lukrative Anlagestrategien. Da wirft dann zum Beispiel ein Herbert Kickl einem Armin Wolf vor, dass dieser als ORF-Moderator verhindern will, dass die österreichische Bevölkerung die „Wahrheit" über eine „geheime" Geldanlageform erfährt, mit der alle „reich" werden können. Oder es sitzt etwa Armin Assinger im Millionenshow-Studio und erklärt in seinem typisch kärntnerischen Dialekt, wie viele auch ohne Millionenshow und auf einfachem Weg zu einem beträchtlichen Vermögen kommen könnten.



ORF-Moderator Armin Wolf warnt in seinem Blog vor Fake-Videos, in denen angeblich Prominente Investmenttipps geben. Foto: Screenshot

Die anschließend folgenden „guten" Tipps sind immer gleich konstruiert. Eine angeblich neue (KI-gesteuerte) Investmentplattform im Internet wird als „exklusiv" präsentiert, ein Link angeboten, über welchen zunächst zahlreiche persönliche Daten wie Vor- und Zuname, Geburtsdatum, Postanschrift, Mobilrufnummer, E-Mail-Adresse, evt. vorhandenes Vermögen u. a. abgefragt werden.

250 Euro als Warnsignal

Dann werden „Erfahrungsberichte" von Personen präsentiert, welche bereits Geld mit dieser Methode verdient hätten und von einer nie versiegenden „Geldquelle" erzählen. Um möglichst viele zum „Investment" zu verleiten, wählen die Täter einen Betrag, den viele Menschen noch rasch zur Verfügung haben und einzusetzen bereit sind. In den allermeisten bisher bekannten Betrugsfällen sind dies – 250 Euro! Vereinzelt wurden auch schon 275 Euro vorgeschlagen. Wer also von solchen Beträgen hört oder liest, bei dem sollten spätestens hier die Alarmglocken laut schrillen.



Foto: AK Tirol

„Politiker und TV-Moderatoren geben keine Anlagetipps. 250 Euro sind ein Alarmzeichen."

Helmuth Lichtmannegger, AK Tirol

Steigende Kurven – alles Fake!

Laufend werden die Opfer dann per Telefon kontaktiert und zu neuen Zahlungen gedrängt. Dabei werden in einer App oder per E-Mail laufend Grafiken präsentiert, welche die „hervorragende Entwicklung" des eingesetzten Kapitals beweisen sollen. Aus den 250 Euro sollen dann innerhalb von wenigen Tagen z. B. 2.500 Euro geworden sein und die Opfer werden aufgefordert, die „Glückssträhne zu nutzen", und zu neuen Geldzahlungen animiert. Will jemand das Kapital oder gar „Gewinne" ausbezahlt bekommen, wird der Kontakt abgebrochen.

Tipps

Investments und Veranlagungen sind interessante, aber auch komplexe Angelegenheiten, die Erfahrung und Wissen erfordern. Versprechungen von sicheren Gewinnen bei null Risiko sollten nirgendwo geglaubt werden.

Wenn Sie bereits in eine solche Falle getappt sind, erstatten Sie Anzeige bei der Polizei und hüten Sie sich vor „Recovery-Betrug": Die Betrüger melden sich Monate später und geben sich als „Helfer" aus, das verlorene Geld „zurückzuholen".



Viele Sicherheitsvorfälle beginnen bei einer Mitarbeiterin bzw. einem Mitarbeiter, daher ist die regelmäßige Schulung in Sachen IT-Sicherheit der Belegschaft unumgänglich. Fotos: iStock

Der Mensch als Sicherheitslücke: Was Arbeitgeber tun müssen

Phishing, Datenlecks, KI-Tools ohne Freigabe: Oft beginnt der Vorfall beim Menschen. Die Verantwortung bleibt meistens beim Arbeitgeber. Was Sie regeln müssen und was Gerichte sagen.

Von Florian Brutter

Ein Klick auf den falschen Link. Eine E-Mail an die private Adresse weitergeleitet. Ein KI-Tool, das niemand freigegeben hat. Viele Sicherheitsvorfälle beginnen bei der Mitarbeiterin oder dem Mitarbeiter, das Problem bleibt der Arbeitgeberin bzw. dem Arbeitgeber. Er muss vorbeugen, schulen und kontrollieren. Und die Kontrolle muss selbst rechtskonform sein. Wer personenbezogene Daten verarbeitet, muss sie durch geeignete technische und organisatorische Maßnahmen schützen und muss dafür sorgen, dass Mitarbeiter mit Zugang diese Daten nur im Rahmen ihrer dienstlichen Aufgaben verwenden und nicht für andere Zwecke. Mitarbeiter müssen vertraglich an das Datengeheimnis gebunden werden, auch für die Zeit nach dem Dienstverhältnis. Zudem müssen Arbeitgeber sie über die geltenden Übermittlungsanordnungen und die Folgen eines Verstoßes belehren.

Seit 1. Oktober 2026 gilt außerdem das NISG 2026. Es setzt die NIS-2-Richtlinie um und erfasst wesentliche und wichtige Einrichtungen, etwa aus Energie, Gesundheit, Verkehr oder Lebensmittelproduktion. Die Leitungsorgane müssen selbst an Cybersicherheitsschulungen teilnehmen. Den Mitarbeitern sind regelmäßig Schulungen anzubieten. Zu den Mindestmaßnahmen zählen Cyberhygiene, Personalsicherheit, Zugriffskontrolle und Multi-Faktor-Authentifizierung. Ob Ihr Unternehmen erfasst ist, hängt von Sektor und Größe ab. Prüfen Sie das jetzt, nicht erst beim ersten Vorfall. Die Wirtschaftskammer bietet dazu einen Online-Ratgeber als Orientierungshilfe an.

Fehler des Mitarbeiters

Ein Datenleck, verursacht durch einen Mitarbeiter, entbindet das Unternehmen nicht von seiner Verantwortung. Eine Pflegepraktikantin postete ein Foto aus der elektronischen Patientendokumentation in ihrer Social-Media-Story. Trotz Schwärzung waren u. a. Vor- und Nachname und eine Pflegemaßnahme erkennbar, es handelte sich also um Gesundheitsdaten. Der Verlust solcher Daten bedeutet in der Regel ein hohes Risiko für den Betroffenen. Melde- und Benachrichtigungspflichten trafen also den Klinikbetreiber als Verantwortlichen, er musste die Patientin informieren. Dass die Praktikantin das Posting nach rund drei Stunden selbst löschte, nutzte nichts mehr. Solche Datenvorfälle müssen unverzüglich, möglichst binnen 72 Stunden, an die Datenschutzbehörde gemeldet werden. Klare interne Meldewege sind daher Pflicht.

Entlassung? Nicht immer

Wer als Mitarbeiter vertrauliche Informationen weitergibt, riskiert die Entlassung. Ein Bauleiter hatte das Anbot eines Konkurrenten dem Unternehmen seiner Lebensgefährtin zukommen lassen. Der OGH hielt die Entlassung wegen Vertrauensunwürdigkeit für vertretbar. Fahrlässigkeit genügt, ein Schaden ist nicht nötig. Für leitende Angestellte gilt ein strengerer Maßstab.

Ein Automatismus ist das aber nicht. Eine Personalmanagerin schickte interne Unterlagen an ihren Lebensgefährten. Dieser ließ sie über einen gesicherten KI-Zugang seines Arbeitgebers übersetzen und zusammenfassen, ohne sie zu lesen oder zu speichern. Das OLG Linz hielt fest: Einer Personalmanagerin ist zuzumuten, vertrauliche Unterlagen auch ohne Kennzeichnung zu erkennen. Einen Geheimnisverrat sah es dennoch nicht. Der Partner sei bloß „Eingabestelle in die Künstliche Intelligenz", also quasi Mittel zum Zweck gewesen. Die KI-Nutzung selbst war ihr nicht als Vertragsverstoß vorgeworfen worden. Die Entlassung war unberechtigt. Für Sie als Arbeitgeber heißt das: Was nicht geregelt ist, lässt sich schwer sanktionieren. Legen Sie fest, welche KI-Tools erlaubt sind und welche Daten hineindürfen. Auch Schadenersatz vom Mitarbeiter ist begrenzt. Für eine entschuldbare Fehlleistung haftet er nicht.



Hacker brauchen sich oft gar nicht anzustrengen, um an Daten von Unternehmen zu gelangen.



Foto: WK Tirol

„Was Sie nicht klar regeln, können Sie im Ernstfall kaum sanktionieren."

Mag. Florian Brutter, Datenschutzbeauftragter der Wirtschaftskammer Tirol

Beim Fake-President-Betrug geben sich Täter als Chef aus. Eine Gruppenleiterin der Finanzbuchhaltung überwies nach 92 gefälschten E-Mails rund 54 Mio Euro. Die Mitarbeiterin verwahrte die TAN-Karten entgegen der Anweisung allein. Davon wusste die Geschäftsführung nichts. Es gab ein Vieraugenprinzip, IT-Richtlinien, Schulungen, Warnmails und einen Social-Engineering-Test. Dass die Mitarbeiterin die Vorgaben umging, war für den Geschäftsführer nicht erkennbar. Die Gesellschaft klagte ihn auf Schadenersatz wegen Verletzung seiner Aufsichtspflichten, aber ohne Erfolg. Geschuldet sei kein Erfolg, sondern eine branchen-, größen- und situationsadäquate Bemühung.

Mitarbeiterkontrollregeln

Schutz braucht Kontrolle, aber nicht jede ist so ohne Weiters erlaubt. Kontrollsysteme, die die Menschenwürde berühren, brauchen eine Betriebsvereinbarung, ohne Betriebsrat ist die individuelle Zustimmung des einzelnen Mitarbeiters nötig. Auch Systeme, die Mitarbeiterdaten über allgemeine Angaben hinaus verarbeiten, sind betriebsvereinbarungspflichtig, wobei schon die objektive Eignung zur Kontrolle zählt, nicht erst die Absicht. Eine bloße Stechuhr berührt die Menschenwürde noch nicht, ein Bewegungsprofil über den ganzen Arbeitstag kann es schon. Zu wählen ist stets das schonendste Mittel, das noch zum Ziel führt. Für Logfiles, E-Mail-Filter oder Überwachungssoftware gilt daher: erst regeln, dann einschalten.

IT-Sicherheit war und ist damit auch eine HR-Aufgabe. Dienstvertrag, IT-Richtlinie, Schulungsplan und Betriebsvereinbarung greifen ineinander. Fehlt ein Baustein, wird es im Ernstfall teuer. Die Behörde fragt nach Ihren Maßnahmen, das Gericht nach Ihrer Dokumentation.

Tipps

So stärken Sie die IT-Sicherheit über Ihre Mitarbeiter:

- Datengeheimnis schriftlich vereinbaren und Mitarbeiter belehren.
- IT- und KI-Richtlinie erlassen: erlaubte Tools, verbotene Daten, Privatnutzung.
- Regelmäßig schulen, Phishing-Tests durchführen, alles dokumentieren.
- Zahlungen nur im Vieraugenprinzip, Kontoänderungen telefonisch rückbestätigen.
- Interne Meldewege für Datenpannen festlegen: Die 72-Stunden-Frist läuft ab Kenntnis.
- Kontrollsysteme vor dem Start mit dem Betriebsrat regeln.
- Prüfen, ob Ihr Unternehmen unter das NISG 2026 fällt. Falls ja: Schulung der Geschäftsleitung einplanen.

Impressum

31. Oktober 2026, KSÖ – Sicher.Tirol

Herausgeber und Medieninhaber: Schlüsselverlag J. S. Moser GmbH; Redaktionelle Betreuung und Layout: Content Studio, Chefredaktion: Lisa Schwarzenauer und Frank Tschoner; Redaktion: hergestellt in Kooperation von Kompetenzzentrum Sicheres Österreich/Landesklub Tirol, Polizei, Tiroler Versicherung, AK Tirol, WK Tirol und Land Tirol; Anschrift für alle: 6020 Innsbruck, Brunecker Straße 3, Postfach 578, Telefon 05 04 03 - 1543.





Das neue Sicherheitszentrum Tirol in Innsbruck, Kapuzinergasse 1, ging mit Oktober 2026 in Vollbetrieb. Fotos: Seidl ARE

Sicherheitszentrum Tirol mit Oktober im Vollbetrieb

Mit der Vollinbetriebnahme des Sicherheitszentrums Tirol sind 19 Organisationsteile der Landespolizeidirektion Tirol und des Innenministeriums von neun Standorten an einem Standort in Innsbruck, Kapuzinergasse 1, vereint. Über 900 Polizeibedienstete arbeiten hier unter modernen Bedingungen.

Im Rahmen einer Pressekonferenz am 20. Oktober 2026 im Sicherheitszentrum im „Saal der Bundespolizei“ wurde vor zahlreichen Medienvertretern die Vollinbetriebnahme als historischer Meilenstein gewürdigt. Innenminister Gerhard Karner, Landeshauptmann Anton Mattle, Landespolizeidirektor Helmut Tomac und die CEO der Austrian Real Estate (ARE) Christine Dornaus informierten gemeinsam über das Projekt und seine Bedeutung für die Sicherheit in Tirol. Dabei wurden die Gebäude am neuen Standort, die Umsetzungsschritte



Landespolizeidirektor Tomac, Innenminister Karner, Landeshauptmann Mattle und die Geschäftsführerin der ARE Dornaus gaben bei der Pressekonferenz Einblicke in das neue Sicherheitszentrum Tirol. Foto: Huter/LPD Tirol

des Bauprojekts sowie die vielfältige Nutzung vorgestellt. Anschließend erhielten die Journalisten bei einem Rundgang im Sicherheitszentrum exklusive Einblicke in die moderne Infrastruktur der dort angesiedelten Organisationseinheiten der Tiroler Polizei.

Das von der Austrian Real Estate (ARE) im Auftrag des Bundesministeriums für Inneres errichtete Sicherheitszentrum Tirol umfasst sieben Baukörper mit rund 56.500 Quadratmetern Nettoraumfläche. Das vom Wiener Architekturbüro Geiswinkler & Geiswinkler geplante Ensemble besteht aus fünf Neubauten sowie zwei generalsanierten und aufgestockten Bestandsgebäuden mit Gesamtbaukosten in der Höhe von ca. 160 Mio. Euro.

Mit der Eröffnungsfeier im Frühjahr 2027 wird das Sicherheitszentrum Tirol dann offiziell seiner Bestimmung übergeben.

Die Mitglieder des KSÖ Tirol

Land Tirol	Landespolizeidirektion Tirol	TYROLIT	Flughafen Innsbruck
Moser Holding	MCI	Tirol Kliniken	Congress-Messe Innsbruck
Arbeiterkammer Tirol	ÖSV	Stadt Innsbruck	Leopold-Franzens-Universität
TIROLER VERSICHERUNG	TIWAG	D. Swarovski KG	Industriellenvereinigung Tirol
Wirtschaftskammer Tirol	UNIQA	Empl Fahrzeugbau	Raiffeisen-Landesbank Tirol AG
Neu seit 2026:	Volksbank Tirol AG	STRONG IT GmbH	

DIE PARTNER DER KOOPERATION:

Tiroler Tageszeitung · AK Tirol · POLIZEI · LAND TIROL · tiroler · WKO Wirtschaftskammer Tirol