HANDELSZEITUNG
NR. 14 | 6. APRIL 2023

SPECIAL
KMU

Cyberangriff: Unternehmen sollten ihre Mitarbeitenden regelmässig schulen, um die Gefahr zu verringern, Opfer eines Cyberangriffs zu werden.

Schutz vor Cyberkriminalität

Bei der **IT-Sicherheit** sollte man sich nicht nur auf die Cyberversicherung verlassen. KMU haben das meiste selbst in der Hand.

MATTHIAS NIKLOWITZ

Phishing im Namen der SBB und Swisspass, falsche Websites, die den Kurierdienst Swissconnect imitieren und Schadsoftware gegen Hotels – das sind die aktuellen Vorfälle, vor denen das Nationale Zentrum für Cybersicherheit (NCSC) gegenwärtig warnt. Pro Woche verzeichnet man hier zwischen 400 und knapp 1000 Meldungen – Tendenz leicht steigend. Die Kategorien Betrug, Phishing und Spam sind mit Abstand am meisten vertreten. Die Zahl der kursierenden Schadprogramme wächst jeden Tag um mehr als 400 000 neue Varianten.

Automatisierung auch bei Attacken

«2021 war mindestens jedes dritte Schweizer Unternehmen Opfer von Cyberkriminalität – und das berücksichtigt nur die gemeldeten Fälle», sagt Nicolas Mayencourt, Gründer und Geschäftsführer des IT-Sicherheitsunternehmens Dreamlab Technologies. Das entspricht einer Verdopplung im Vergleich zum Jahr 2020. «Der durchschnittliche Schaden durch eine Cyberattacke für ein KMU beläuft sich auf mehrere hunderttausend Franken. Schwere Angriffe mit Datendiebstahl und -verschlüsselung verursachen Schäden im zweistelligen Millionenbereich.» Mit dieser Dynamik hält das Verhalten der Unternehmen nicht Schritt, so Mayencourt. «Viele KMU verfügen über wenig Ressourcen oder sehen sich nicht als potenzielles Ziel.»

Angriffe würden heute professionell und hochgradig automatisiert ausgeführt. So sieht sich ein KMU mit denselben Angreifenden und Angriffsmethoden konfrontiert wie ein internationaler Grosskonzern, sagt Mayencourt weiter. «Generell erkennen wir eine Verlagerung der kriminellen Aktivitäten hin zu wenig geschützten Zielen.» Ransomware-as-a-Service-(RaaS-)Angebote seien sehr populär geworden. Diese ermöglichen es, selbst Ransomware-Angriffe zu starten – ohne grosse technische Kenntnisse. Die RaaS-Kits können für wenige hundert Franken mit Rund-um-die-Uhr-Support im Dark Web gemietet werden. «Zunehmend geraten auch gesamte Lieferantenketten ins Visier der Kriminellen», so Mayencourt. Auch mit künstlicher Intelligenz (KI) würden tückische neue Angriffstechniken kreiert: Deepfakes gaukeln durch Bilder, Audio- und Videofälschungen täuschend echte Inhalte vor. «Hinzu kommen Taktiken wie das Voice Cloning, welche bewirken, dass Computer wie echte Menschen klingen», so Mayencourt. «Dabei imitieren die Angreifenden beispielsweise die Stimme eines Vorgesetzten.»

«KMU müssen sich in erster Linie selbst schützen», rät Mayencourt, der zum Thema auch ein Buch verfasst hat. «Guter Schutz ist nicht teuer und fängt bei der Belegschaft an.» Der Mensch sei der entscheidende Faktor in der Gleichung. Die KMU müssten ihre Mitarbeitenden sensibilisieren und befähigen, mit Cyberrisiken achtsam umzugehen. «Gut geschulte Mitarbeitende werden somit nämlich zur stärksten Waffe im Kampf gegen Cyberkriminalität.» Auch die öffentliche Hand müsse zumindest einen Teil der Verantwortung übernehmen. «Insbesondere im öffentlichen Raum muss ein Regelwerk definiert werden, welches unsere Handlungen, Rechte und Pflichten – ähnlich wie beispielsweise im Strassenverkehrsgesetz – regelt», meint Mayencourt. «Wenig hilfreich wäre eine Cyberversicherung als alleiniger Rettungsanker. Diese würde falsche Anreize in Bezug auf Eigenverantwortung setzen.»

Mayencourt hat eine Reihe von Tipps zur Hand, mit denen KMU ihre Risiken, Opfer von Cyberkriminalität zu werden, massiv senken. Ein erster Schritt ist das Sensibilisieren und Schulen der Mitarbeitenden für die Gefahr. Dann muss die Software stets auf dem neusten Stand gehalten werden. Weiter empfiehlt sich das Verwenden eines Passwortmanagers, um Passwörter zu erstellen und abzurufen. Hierzu gehört auch, falls möglich, das Aktivieren der Zwei-Faktor-Authentifizierung. Wichtiges weiteres Element ist das Nachdenken, bevor auf einen Link geklickt oder Anhänge geöffnet werden. Ergänzend hinzu kommt der Hinweis, nicht auf unsicheren Websites zu
das Vorhängeschloss-S
ten, denn: HTTPS
Verschlüsselun
zwischen den
den Websit
100-Proze
fang. Un
relevant
«Ideale
welche
aufbew

KI vert

«Die
und Ma
eins», so
tenden di
sicherheit
Umgang mit

KI und mas
gemäss Mayenco
tionssicherheit imme
Technologien lernen und ve
ständig, da sie mit riesigen Datenmengen gefüttert werden», beschreibt Mayencourt diese Entwicklung. «Einfach ausgedrückt: Menschen sind nicht in der Lage, die Komplexität unserer hypervernetzten Welt zu überblicken. Die KI schon und hat damit grosses Potenzial und wird vieles in der Zukunft revolutionieren. Das muss aber aufgrund ihrer enormen Leistungsfähigkeit im Sinne der Gesellschaft gesteuert passieren.»

Chat GPT: Freund oder Feind?

IT-Sicherheit Ob und in welchem Ausmass Chat GPT und ähnliche KI-Systeme Jobs überflüssig machen werden, ist derzeit noch offen. Fest steht: IT-Sicherheitsleute werden weiterhin gebraucht werden. Denn Chat GPT und Co., die ursprünglich auch dafür entwickelt worden sind, Computercodes selbstständig zu erstellen, können auch sogenannte polymorphe Software entwickeln, mit der sie kaum noch entdeckt werden. Als Trainingsmaterial wird hier dann einfach der Code verwendet, der auf den einschlägigen Marktplätzen im Darknet erhältlich ist. Auch das Hochladen von firmeneigenen Daten für das Training der Systeme kann kritisch sein, wenn dazu sensible Informationen gehören. Chat GPT kann indes auch die Cybersicherheitsindustrie verändern und rascher Hacker-Attacken entdecken, schneller auf Angriffe reagieren und die Entscheidungsfindung verbessern. Ob Chat GPT Freund oder Feind ist, ist derzeit laut Experten noch offen.

Reach
58,000
readers

SME special edition

What are the top topics for Swiss SMEs in 2023? Trends and solutions in the «Handelszeitung» national special on 31 August 2023

Ringier | Advertising

Characteristics

Switzerland is a country of SMEs. There are almost 600,000 small and medium-sized enterprises in the Swiss Confederation. This means that 99.7% of companies in Switzerland are considered SMEs; according to the definition, they employ fewer than 250 people.
The 2023 SME specials in «Handelszeitung» are dedicated to issues that are of particular interest to small and medium-sized enterprises in Switzerland. They analyse the challenges and opportunities for SMEs from different perspectives, as well as highlighting current trends and possible solutions.

What are the top topics for Swiss SMEs in 2023? How is the digital and sustainable transformation of the Swiss economy impacting small and medium-sized enterprises? What innovative solutions are available to alleviate the shortage of skilled workers? Readers can find answers to these questions in the informative «Handelszeitung» special on 31 August 2023.

**Book your ad in this national special online now – you can also arrange its renewal at the same time.
All «Handelszeitung» specials are also published digitally at handelszeitung.ch/specials!
We will be happy to advise you.**

Publication date

Topic	Published	Advertisement deadline	Print material deadline
SME	31.08.2023	17.08.2023	28.08.2023

Pricing

Page format	Width x height mm	Gross price CHF 4c
1/1 page	291 x 438	13 500
Junior Page Mini	173 x 250	6 954
Junior Page Maxi	232 x 300	10 173
1/2 page, landscape	291 x 219	8 505
2/5 page	114 x 438	6 664
1/3 page, landscape	291 x 145	5 631
1/4 page, landscape	291 x 110	4 272
1/5 page, portrait	114 x 219	4 950

Other formats are available on request

Further planned specials with focus on SMEs

Topic	Title	Published
Top 100 Startup	Handelszeitung PME	07.09.2023 27.09.2023
The Spirit of Bern	Handelszeitung	07.09.2023
Top innovations	Bilanz PME	29.09.2023 27.09.2023
Basle Area	Handelszeitung	12.10.2023
Marketing (GfM)	Handelszeitung	26.10.2023
Legal guide	Handelszeitung	02.11.2023
Riskmanagement	Handelszeitung	02.11.2023
Central Switzerland	Handelszeitung	16.11.2023

Online

All «Handelszeitung» specials are now also published online at handelszeitung.ch/specials. We offer exciting advertising opportunities and formats.

Expand your reach to include our online audience.
We will be happy to advise you in detail.

Conditions
Advertising rates valid from 01/01/2023. All prices in CHF/gross, AC YTP 15% plus 7.7% VAT. Prices subject to change. The general terms and conditions apply, and can be found at www.ringier-advertising.ch.

Key figures	**Handelszeitung**
Distributed circulation:	31,607 copies
Readership:	58,000 readers
Reach:	1,2%
Men/women:	73%/27%

Sources: WEMF-Circulation Bulletin 2022 and MACH Basic 2023-1, German-speaking Switzerland

Contact
Ringier Advertising

Michael Germann
michael.germann@ringier-advertising.ch
Tel. +41 44 259 89 63

Delivery of print material
anzeigen-prod@ringier.ch