RegionalWirtschaft

Zürcher Oberländer Anzeiger von Uster

Das Wirtschaftsleben in der Region

Freitag, 12. März 2021

Homeoffice-Blues 5
Lea Keller-Ruckstuhl von der Fachstelle Sucht Bezirk Hinwil warnt vor Suchtgefahren.

Private Schulden 7
Ein regionales Inkassobüro äussert sich zur Zahlungsmoral während der Krise.

Erfolg mit Hygiene 9
Die Pfäffiker Firma Sorein hat ein Desinfektionsmittel entwickelt – in Rekordzeit.

Der gute Hacker

Mit simulierten Cyberangriffen deckt Ivan Bütler Schwachstellen von IT-Systemen schonungslos auf: Der Chef von Compass Security in Rapperswil-Jona erzählt im Interview, wie Kriminelle auf vertrauliche Firmendaten zugreifen und sie zu Geld machen, welche neuen Gefahren durch die Pandemie entstanden sind und was wir aus den jüngsten Angriffen auf Oberländer Konzerne lernen können.
Seiten 2/3

Foto: Seraina Boner

Ein Bruder für den Uster-Batzen

Wetzikon Um das lokale Gewerbe zu unterstützen, wollen Wetziker Wirtschaftsvertreter zusammen mit der Stadt Wetzikon ein neues Zahlungsmittel entwickeln: den «Wetzikoin» (ein Wortspiel mit dem englischen «coin» für Münze). Er ist als digitales Pendant zum physischen Glatttaler oder Uster-Batzen gedacht. Die Bezahlung würde rein digital über eine bereits existierende Schweizer App erfolgen. «Einmal gekauft, kann der Wetzikoin in ganz Wetzikon wie Bargeld eingesetzt werden», schreibt das Wirtschaftsforum Wetzikon in einer Mitteilung an seine Mitglieder, die dem ZO/AvU vorliegt.

Ebenfalls in das Projekt involviert sind der Gewerbeverein Wetzikon sowie die weiteren Mitglieder der IG Netzwerk Standortförderung (VWO, Wetzikontakt und IG Bildung). Sie begründen ihr Anliegen auch mit Verweis auf die vom Stadtrat Wetzikon lancierte E-Coupon-Aktion, deren Umsetzung durch den zweiten Lockdown begrenzt worden sei. *jöm*

Impressum

RegionalWirtschaft – ein Produkt der Zürcher Oberland Medien AG

Redaktion: Jörg Marquardt, Manuel Reimann (Produktion)

Verkauf: Marcel Hofer (Leitung), Viviane Andres, Hannes Frei, Jeannette Kammermann, Susi Pulver, Ilona Steiner, Christine Vogt

Abonnemente: Susanna Limata (Leitung)

Kontakt: Redaktion: Tel. 044 933 33 33, regionalwirtschaft@zol.ch

Verkauf: Tel. 044 933 32 04, inserate@zol.ch

Schwerpunkt

«Mitarbeiter werden zu unfreiwilligen Handlangern der Hacker»

Höhere Verwundbarkeit: Aus Sicht von Profihacker und Cyber-Security-Experte Ivan Bütler hat der jüngste Digitalisierungsschub neue Angriffsflächen im Internet geschaffen.

Rapperswil-Jona Ivan Bütler ist der Hacker, dem die Firmen vertrauen. Der Chef von Compass Security hilft ihnen, Cyberkriminelle abzuwehren. Ein Interview über neue Gefahren, verführerische Geschichten und unmoralische Angebote.

Ivan Bütler ist ein Profihacker, aber einer von den Guten. Wenn der Chef von Compass Security in Rapperswil-Jona in das Computernetzwerk von Firmen einbricht, dann nur auf deren Wunsch. Bütler unterzieht die IT-Infrastruktur seiner Kunden einem strengen Stresstest. Er zeigt auf, wie leicht Schadprogramme installiert und geheime Daten erbeutet werden können.

«Ethical Hacking» nennt er seine Tätigkeit, weil er Firmen für die Gefahr von Cyberkriminalität sensibilisiert – und ihnen hilft, sich dagegen zu schützen.

Fahren Sie einen gepanzerten Wagen, Herr Bütler?
Ivan Bütler: Nein, nein, so paranoid bin ich noch nicht.

Aber Sie leben gefährlich, oder? Immerhin pfuschen Sie Cyberkriminellen ins Handwerk.
Es gab schon brenzlige Fälle, wo ich als Berater hinzugezogen wurde. Dabei ging es um die Aktivitäten fremder Geheimdienste oder rechtsextremer Netzwerke. Näheres darf ich dazu nicht sagen. In erster Linie arbeite ich aber für die Wirtschaft. Meine Auftraggeber wollen, dass ich Schwachstellen in ihrer IT-Infrastruktur aufspüre und schliessen helfe. Als gefährlich empfinde ich meine Arbeit daher nicht.

Wer hackt Firmen: eine Bande von Gangstern in abgedunkelten Hinterzimmern?
Von solchen Hollywood-Illusionen müssen wir uns verabschieden. Die Hacker sind nur das Werkzeug, damit der Rubel rollt. Cyberkriminalität ist ein Business-Case. Nehmen wir die Quartalsabschlüsse...

... die von den börsenkotierten Firmen publiziert werden.
Es gibt Netzwerke, die sich auf Insider-Handel spezialisiert haben. Vor der Publikation verschaffen sie sich Zugriff, um mit den Daten Geschäfte zu machen, sei es, dass sie sie verkaufen oder selber für Spekulationen an der Börse nutzen. Die Hacker brechen in die Computersysteme ein und geben die Daten an ein Team weiter, das die Quartalsabschlüsse auswertet.

> «Ich bin auch Familienvater und will meinen Status nicht aufs Spiel setzen.»

Wo sitzen die Hacker?
Vor allem in Russland, China und den USA. Prädestiniert für Cyberkriminalität sind Länder mit guter Ausbildung und hoher Arbeitslosenquote. Ich denke auch an Südamerika, wo bereits eine Kultur der Mafia existiert. Für junge Menschen dort ist Hacking ein lukratives, aber ungefährliches Geschäft.

Apropos: Haben Sie unmoralische Angebote erhalten?
Und?
Natürlich habe ich abgelehnt. Mal abgesehen davon, dass ich so etwas ethisch falsch finde, bin ich auch Familienvater und will meinen Status nicht aufs Spiel setzen.

Der wirtschaftliche Schaden von Cyberkriminalität ist immens: Experten haben ihn 2019 auf 520 Milliarden Euro weltweit pro Jahr beziffert. Fünf Jahre zuvor waren es noch 385 Milliarden Euro.
Wir sind enorm verwundbar geworden. Die Komplexität des Internets, der Zuwachs an Optionen und der Reifegrad der Technologien machen es Kriminellen aktuell leicht, ein Schadprogramm zu installieren und Daten abzugreifen. Es gibt Hacker, die Privatpersonen mit simplen Mitteln erpressen, etwa indem sie behaupten, kompromittierende Daten zu besitzen. Damit lassen sich aber keine grossen Beträge erbeuten. Profis gehen viel gezielter vor.

Solche Profis haben Mitte Dezember 2020 den Pfäffiker Verkabelungsspezialisten Huber+Suhner angegriffen. Laut dem Konzern gab es zwar keinen Datendiebstahl, aber es kam zu einem Produktionsunterbruch und Lieferverzögerungen. Kennen Sie den Fall?
Ich bin mit meiner Firma oft in solche Fälle involviert. Sie zeigen, dass Datensicherheit ein Prozess ist. So wie wir unsere Handys updaten, sollten Firmen auch ihre Sicherheitssysteme laufend überprüfen und aktualisieren.

In den Medien war von «Ransomware-Banden» die Rede, denen Huber+Suhner zum Opfer gefallen sein soll. Bei Ransomware werden Daten verschlüsselt und nur gegen Zahlung eines Lösegelds wieder freigegeben.
Ransomware ist nur einer von vielen Business-Cases der Cyber-Kriminellen. Je mehr Daten über einen längeren Zeitraum verschlüsselt worden sind, umso grösser der Druck zu zahlen. Deshalb greifen viele Kriminelle die Sicherheitskopien von wichtigen Firmendaten an, wenn sie sich Zugang zum Backup-Ordner verschaffen konnten.

Warum genau?
Weil solche Angriffe über einen längeren Zeitraum oft unbemerkt bleiben. Firmen machen sich oft zu wenig Gedanken über die Anzahl der Backups und deren Verwahrung. Sie merken dann zu

Foto: Seraina Boner

griff mit gefälschten E-Mails, die die Einladung zu einem Klassentreffen suggerierten. Einige Mitarbeiter waren so neugierig, dass sie einen Link anklickten. Damit hatten wir Zugriff auf ihr E-Mail-Konto – und von dort auf den Server der Bäckerei. Mit plausiblen Geschichten werden Mitarbeiter zu unfreiwilligen Handlangern der Hacker.

Wie reagieren die Firmen, wenn Ihnen so etwas gelingt?
Diejenigen, die sich zum ersten Mal durch Profis in einem simulierterten Test angreifen lassen, sind oft völlig überrascht. Aber ein Antivirus-Programm allein bietet eben keinen ausreichenden Schutz. Wenn wir ein halbes Jahr später einen Re-Check machen, sind die Kunden in der Regel viel besser gerüstet. Mit der Zeit identifizieren wir kaum noch Schwachstellen oder nur solche, die viel Aufwand für die Täterschaft bedeuten.

Ist das Risiko von Cyberangriffen während der Pandemie grösser geworden?
Auf jeden Fall. Die Pandemie hat einen enormen Digitalisierungsschub ausgelöst. Dadurch werden die nötigen Qualitätsstandards bei der Sicherheit oft nicht zu 100 Prozent eingehalten. Die Verwundbarkeit hat zugenommen.

Welche Angriffe sind typisch?
Wir haben kürzlich eine Firma betreut, die sich einen Trojaner in der Büroanwendung Office 365 eingefangen hatte. Das Schadprogramm war in der Lage, die Zwei-Faktor-Authentifizierung zu umgehen und E-Mails im Namen des CEOs zu versenden. So etwas ist natürlich sehr gefährlich, weil aktuell sehr viele Unternehmen auf diese Anwendung wechseln.

Im Homeoffice greifen Mitarbeiter über ein «Virtuelles Privates Netzwerk» (VPN) auf das Firmennetz zu. Was bedeutet das für die IT-Sicherheit?
Dass die Zeiten vorbei sind, wo man mit einer Firewall eine Burgmauer um die Firma ziehen konnte.

Dann hat Ihnen die Pandemie sicher ein noch volleres Auftragsbuch beschert.
Nicht sofort. Wir bewegen uns in einem Investitionsbusiness. Unsere Kunden nehmen Geld in die Hand, um ihre Sicherheitsarchitektur zu testen und notfalls zu verbessern. Zu Beginn der Pandemie hatten wir weniger Aufträge, weil Firmen sich mit Investitionen zurückhielten. Aber schon bald zog die Nachfrage wieder deutlich an. Momentan sind wir extrem gut ausgelastet.

Ist das Problembewusstsein für die eigene Verwundbarkeit gestiegen?
Grosse Firmen wie Banken und Versicherer sind sich der Risiken seit Langem bewusst und treffen aufwendige Vorkehrungen, um sich zu schützen. Aber auch KMU sind inzwischen sensibilisiert. Praktisch jeder kennt eine Firma, die es erwischt hat.

Wo liegt der Schwerpunkt bei Ihren Kunden?
An uns wenden sich grosse Konzerne genauso wie KMU. Es gibt auch keinen Fokus auf bestimmte Branchen. Die zentrale Frage lautet: Wie lassen sich Daten von Hackern monetarisieren? Was ist der Business-Case?

Sie nannten die Quartalszahlen, die sich kriminell nutzen lassen. Welche «Business-Cases» gibt es noch?
Beliebte Angriffsziele sind Firmen mit «Payment Gateways», sprich: Software-Plattformen zur Abwicklung von Zahlungsprozessen. Dort können sich Hacker direkt bereichern. Genauso gefährdet sind Industrieunternehmen auf Expansionskurs. Deren Mitbewerber könnten sich mit dem Kauf geklauter Daten einen Wettbewerbsvorteil und Zugang zu geistigem Eigentum verschaffen. Bevor wir das Sicherheitssystem eines Kunden testen und ihn hacken, müssen wir zuerst analysieren, wo ein Angriff am meisten wehtun würde.

Wenn sich selbst grosse Firmen nicht vor Cyberangriffen schützen konnten, wie wollen Sie dann KMU davon überzeugen, in ihre IT-Sicherheit zu investieren?
Bei den kleineren Firmen spüre ich tatsächlich eine gewisse Verunsicherung. Aber das heisst nicht, dass sie die Hände in den Schoss legen. Viele sind mit einem KMU-Grundschutz gegen Cyberangriffe versichert. Dafür müssen sie einen Mindeststandard erfüllen. Es ist wie beim Auto: Einmal im Jahr sollte man zum Service.

Ist Ihre Firma auch schon Opfer eines Angriffs geworden?
Vor einiger Zeit hat jemand aus unserer Administration eine E-Mail mit Schadsoftware erhalten und den Link darin angeklickt. Zum Glück wurde der Fehler schnell bemerkt. Wir haben den betroffenen Laptop rechtzeitig vom Netz genommen, bevor das Programm auf unser System übergreifen konnte. Der Laptop war dann aber verloren.

Interview: Jörg Marquardt

spät, dass ihre Daten unbrauchbar geworden sind.

Sollten sie auf die Lösegeldforderung eingehen?
Die Polizei und die Melde- und Analysestelle Informationssicherung Melani raten davon ab. Es gibt aber oft Fälle, wo die Lösegeldsumme niedriger ausfällt als der zu erwartende Schaden. Dann ist die Zahlungsbereitschaft bei den betroffenen Firmen erwartungsgemäss hoch.

Das ist doch ein fatales Signal an Wirtschaftskriminelle.
Ich sehe das Vorgehen auch zwiespältig, weil so das Erpressungsbusiness am Laufen gehalten wird.

Können Firmen überhaupt davon ausgehen, dass sie nach einer Zahlung die volle Datenhoheit zurückgewinnen?
Eine Garantie haben sie nicht. Die Firmen sollten aber in jedem Fall sicherstellen, dass das Einfallstor, durch das der Angriff erfolgt war, wieder verschlossen ist.

Was sind die Haupteinfallstore?
Es gibt die technische und die menschliche Ebene. Bei IP-gestützten Systemen besteht die Gefahr, dass Serverdaten von aussen manipuliert werden. Ein Programmierer ist gut darin, eine Abweichung in der Sicherheitsarchitektur festzustellen, mit der er rechnet. Aber unerwartete Manipulationen übersieht er leicht. Die andere Achillesferse ist die Anfälligkeit der Menschen für gute Geschichten.

> «Die Zeiten sind vorbei, wo man eine Burgmauer um die Firma ziehen konnte.»

Gute Geschichten?
Ein Beispiel: Eine grosse Bäckerei hat uns beauftragt, ihr Sicherheitssystem zu testen. Wir starteten dann einen Phishing-An-

Am Dienstag, den 23. März referiert Ivan Bütler am 42.Top-Anlass des Wirtschaftsforums Uster über das Thema «Industrie 4.0: Ein leichtes Spiel für Hacker». Der Vortrag beginnt um 18.30 Uhr und findet virtuell statt. **Weitere Informationen und Livestream unter: www.wfu.ch.**

Zur Person

Ivan Bütler (50) ist Gründer und Geschäftsführer von **Compass Security** mit Sitz in **Rapperswil-Jona**. Das IT-Unternehmen gehört zu den führenden Schweizer Anbietern im Bereich der Prävention und Aufklärung von Cyber-Attacken. Es beschäftigt rund 60 Mitarbeiter an den Standorten Jona, Zürich und Bern sowie in Berlin und Toronto. Bütler hat sich international einen Namen als Experte für Cyber-Security gemacht und tritt mit einschlägigen Publikationen und Vorträgen an die Öffentlichkeit. Er unterrichtet an der Fachhochschule Rapperswil und an der Hochschule Luzern. *jöm*

Ticker

8. März: BSU-Bilanzsumme erreicht Schwelle von 1,1 Milliarden

Uster Die Bank BSU mit Sitz in Uster hat ihr Geschäftsergebnis bekannt gegeben. Trotz des tiefen Zinsniveaus konnte sie den Zinsertrag mit 12,4 Millionen Franken halten. Beim Zinserfolg vermeldet die Bank eine Verbesserung um 5,9 Prozent – dies aufgrund der tieferen Refinanzierungskosten, wie aus der Medienmitteilung hervorgeht. Mit einem Anteil von 80 Prozent am Gesamtertrag bleibe das Zinsgeschäft «der mit Abstand stärkste und wichtigste Ertragspfeiler».

Die Bilanzsumme erhöhte sich um 58 Millionen Franken oder 5,5 Prozent. Dadurch werde nun die Schwelle von 1,1 Milliarden Franken bei der Bilanzsumme erreicht. Der Bestand an Kundenausleihungen verbesserte sich gegenüber dem Vorjahr um 46,8 Millionen Franken oder 5,2 Prozent auf 944,9 Millionen Franken. Der Anteil der Festhypotheken am Gesamtbestand der Ausleihungen beträgt 93,6 Prozent.

Bei den Kundengeldern verzeichneten die Geschäftsstellen in Uster, Dübendorf und Volketswil einen Zuwachs von 25,7 Millionen Franken. Der Geschäftserfolg liegt mit 2,1 Millionen Franken um 6,9 Prozent über dem Vorjahr. *zo*

2. März: Verteidigungssegment stützt Elma Gruppe

Wetzikon Die Elma Gruppe publiziert ihr Jahresergebnis 2020. Trotz verbesserter Profitabilität verzeichnet der Wetziker Hersteller von Electronic-Packaging-Produkten sowohl beim Bestellungseingang (-3,6 Prozent) als auch bei den Nettoerlösen (-2,7 Prozent) einen Rückgang.

Der Bestellungseingang verringerte sich von 159 Millionen Franken im Vorjahr auf 153,3 Millionen. Während in Asien die Bestellungen um 12,4 Prozent zunahmen, gingen sie in den Regionen Americas (-3,9 Prozent) und Europe (-5,7 Prozent) zurück. Rechnet man die Währungseffekte heraus, kann Elma für den Bestellungseingang insgesamt ein leichtes Plus ausweisen. Die unverändert gute Nachfrage im Verteidigungssegment hat laut Medienmitteilung zur «erfreulichen Entwicklung» beigetragen.

Bei den Nettoerlösen belief sich der Rückgang auf 4,2 Millionen Franken: von 151,2 auf 147 Millionen Franken. Dafür macht Elma die schwächere Wirtschaftsdynamik in Deutschland, Frankreich und Grossbritannien und damit verbundene Projektverzögerungen verantwortlich. Für die USA und Asien vermeldet die Gruppe dagegen eine Steigerung des Gesamtumsatzes.

Elma schliesst das Geschäftsjahr mit einem Gewinn von 5,6 Millionen Franken ab (Vorjahr: 5,1 Millionen). Auch das Betriebsergebnis vor Zinsen und Steuern (Ebit) lag mit 6,6 Millionen Franken oder 4,5 Prozent leicht über dem Vorjahr (6,4 Millionen Franken oder 4,2 Prozent). *jöm*

4. März: Neuorganisation bei Richard Gartenbau

Wetzikon Die Richard Gartenbau AG in Wetzikon organisiert sich neu: Inhaber Erhard Diener übergibt seine Aufgaben in jüngere Hände. Neben dem Sohn Roger Diener, der das Geschäft bereits seit zehn Jahren führt, wird Philipp Wälty als stellvertretender Geschäftsleiter neu die operativen Arbeiten des Vaters weiterführen. Wälty ist diplomierter Bauführer.

Laut Medienmitteilung arbeitet Erhard Diener im Hintergrund mit einem reduzierten Pensum weiter und verbleibt auch im Verwaltungsrat der Firma, um sein Wissen weiterhin einzubringen und das Team zu unterstützen. Er war insgesamt 34 Jahre für die Gartenbaufirma tätig, davon zwölf Jahre als deren Inhaber. Zu den von ihm verantworteten Projekten gehören etwa der General-Guisan-Quai in Zürich oder die Aussensportanlage Buchholz in Uster. Die im Oberland und im Raum Zürich tätige Firma besteht seit 90 Jahren und beschäftigt 40 Mitarbeiter. *zo*

9. Februar: Neue Führung bei R&M in Amerika

Wetzikon Der Verkabelungsspezialist Reichle & De-Massari (R&M) aus Wetzikon vermeldet zwei Neubesetzungen auf Führungsebene. Per 1. Februar wurde der langjährige Senior Manager Paulo Campos zum neuen Executive Vice President für die Geschäftseinheit Americas und Managing Director R&M USA, Inc. ernannt. In den letzten sechs Jahren hat er das Unternehmen laut Medienmitteilung erfolgreich in Lateinamerika etabliert. Dazu gehörte auch der Aufbau einer eigenen Produktionsstätte. «In dieser Zeit wurde R&M zu einem der führenden Player in Brasilien», heisst es in der Mitteilung.

Als neuer Managing Director übernimmt Edison Castro die Verantwortung für die Geschäftseinheit Südamerika. Castro hatte in den letzten 15 Jahren verschiedene Senior-Management-Positionen in der Industrie inne, wie es in der Mitteilung heisst. Zuletzt war Edison Castro Sales Director für die Region Lateinamerika im Multimedia-Solutions-Geschäft von Prysmian.

R&M bezeichnet Nord- und Südamerika als wichtige strategische Wachstumsmärkte für R&M und sieht die Ernennung der beiden Senior Manager im Zusammenhang mit seiner Wachstumsstrategie in dieser Region. *zo*