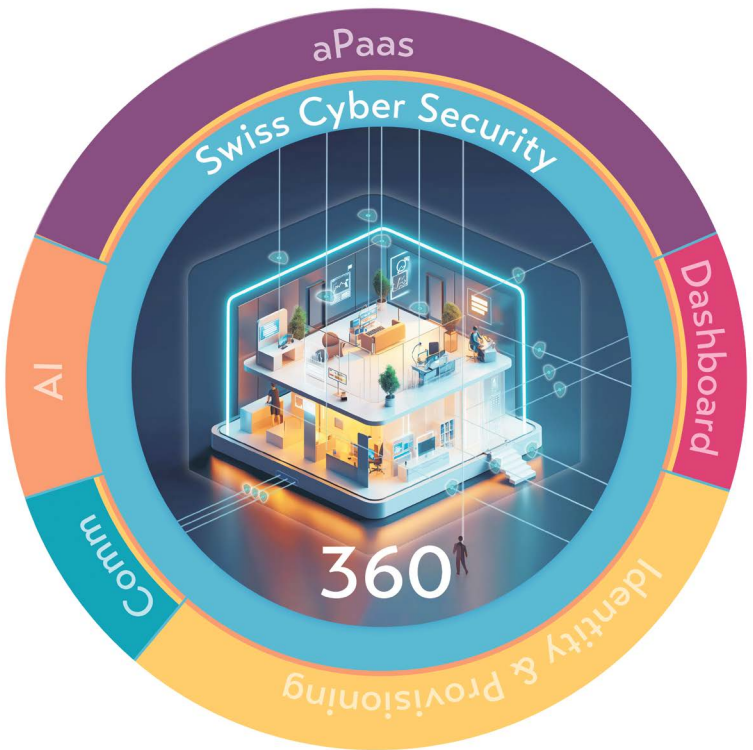
«Verlust von Datenkontrolle ist existenzbedrohend»

Firmen müssen Cybersecurity gewährleisten und dabei effizient und wirtschaftlich arbeiten. Mit AGON gelingt dieser Spagat.

Herr Gurtner, was hält Schweizer Unternehmer*innen nachts wach, wenn es um Cybersicherheit und Resilienz geht?
Tobias Gurtner: Eine Verwaltungsrätin, ein Geschäftsleitungsmitglied oder ein ITler haben schlaflose Nächte, wenn es oft zu spät ist: Der Supergau, sprich der Verlust der Kontrolle über Daten, ist Realität. Also muss man antizipieren! Nach 25 Jahren Tätigkeit kann ich sagen: Ein Fünf-Mann-Betrieb verfügt über die gleichen Painpoints wie ein Konzern mit 5000 Mitarbeitenden. Warum? Der leichteste Weg, um ein System zu knacken, führt immer über eine Person vor dem PC. Der Zugang zu einem System stellt fast immer den «entscheidenden» Sicherheitsfaktor dar.

Was bietet AGON Partners gegenüber einer so menschlichen Gefahr?
Tobias Gurtner: Unsere Geschäftssparte «Swiss Cyber Security» hat sich durch die enge Zusammenarbeit mit führenden Technologieanbietern als verlässlicher Partner für fortschrittliche Cybersecurity-Lösungen etabliert. Für unsere Kunden stellen wir – nach Analyse der bestehenden IT-Umgebung – aus unserem IT-Werkzeugkasten den optimalen Cyber-Schutz zusammen. Dieser erstreckt sich von phishingresistenten Multi-Faktor-Authentifizierungen bis hin zu KI-gestütztem Identitäts- und Zugriffsmanagement. Dabei richten wir uns nicht nur nach den aktuellen Sicherheitsanforderungen, sondern blicken auch in die Zukunft. Unsere Mitarbeitenden versuchen Entwicklungen aufzugreifen, bevor diese grossflächig von Cyber-Kriminellen eingesetzt werden.

Benötigt man hierfür von Kundenseite entsprechendes IT-Know-how?
Tobias Gurtner: Nein. Wichtig ist, dass sich die Unternehmensführung darüber im Klaren ist, was die Firma benötigt. Unsere KI-basierte Evaluation setzt bei den Sicherheitslücken an, analysiert u.a. die bestehende IT-Infrastruktur und antizipiert künftige Anforderungen des Unternehmens an den Cyber-Schutz. Unser Evaluations-Tool informiert VR und GL dabei umgehend über die Kosten, welche erforderlich sind, um die Sicherheitslücken zu schliessen. Wir bei AGON unterscheiden somit die strategische Ebene und in der Folge die operative Umsetzung. Dort arbeiten unsere IT-Spezialisten eng mit den IT-Cracks der Kunden zusammen.



Unternehmen, welche die vollen 360 Grad an Sicherheit abdecken wollen, müssen auf verschiedene Themenfelder achten. Grafik: ZVG

Sie haben erwähnt, dass beim Identitäts- und Zugriffsmanagement auch KI zum Einsatz kommt. Wie relevant ist künstliche Intelligenz in Ihrem Feld?
Tobias Gurtner: Unsere Mitarbeitenden faszinieren sowohl die enormen Chancen als auch die Gefahren dieser disruptiven Technologie. Wir werden zum Beispiel im Bereich Social Engineering eine Verschärfung der Lage sehen, da sich durch die Nutzung von Deepfakes ganz neue Betrugsmodelle eröffnen. Unsere KI-gestützten Lösungen ermöglichen es, in Echtzeit potenzielle Bedrohungen zu identifizieren und auf sie zu reagieren. Durch die kontinuierliche Überwachung und das schnelle Erkennen von Anomalien bieten wir unseren Kunden eine proaktive Sicherheitsstrategie, die sich laufend an die dynamischen Herausforderungen der digitalen Welt anpasst.

Welche Sicherheitsthemen sehen sie mittel- bis langfristig auf Schweizer Unternehmen zukommen?
Patrick Krauskopf: Als Präsident zahlreicher (auch börsenkotiert) Unternehmen ist für mich klar, dass die Cyber-Gefahren meine Unternehmen in ihrer schieren Existenz gefährden können. Wenn ich mit meinem CEO bei AGON Partners spreche, wird mir das Ausmass dieser Gefahren oft erst richtig bewusst. Meine Geschäftsleitungen müssen in der Lage sein, präventive Massnahmen zu ergreifen und sicherzustellen, dass das Unternehmen bestens auf Worst-Case-Szenarien vorbereitet ist. Im Austausch mit anderen Unternehmensführern stelle ich aber immer wieder fest, dass dieses Bewusstsein – gerade bei KMU – oft fehlt. Die Kontrolle über unternehmerische Daten ist die zentrale Herausforderung im Bereich Compliance geworden. Als Professor für Wirtschaftsrecht und Compliance muss ich deswegen auch den Akzent in der Weiterbildung ändern.

Welche Möglichkeiten gibt es Ihres Erachtens?
Patrick Krauskopf: Die Lösung liegt in einem Cybersecurity-Ansatz, der die unternehmerischen Prozesse nicht blockiert und für die Entscheidungsträger der Firma kontrollierbar ist. Denn schliesslich möchte man sich weder in eine Abhängigkeit zu einem Provider noch zur eigenen IT begeben. Und zu guter Letzt sollte die Lösung auch kostentechnisch tragbar sein. Darum haben wir mit AGON Partners Innovation ein Unternehmen im Markt positioniert, das den Bedürfnissen von KMU bis hin zu börsenkotierten Grossbetrieben entsprechen kann: ein Schweizer Unternehmen mit hiesigen Mitarbeitenden, das für seine Kunden Schweizer Datenhoheit sicherstellt. Dass wir Ständerätin Brigitte Häberli-Koller als Verwaltungsrätin an Bord haben, macht uns zusätzlich stolz!

Tobias Gurtner, Jahrgang 1980, ist ein erfahrener Cybersecurity-Spezialist, Leiter des Software- und Applikationsentwickler-Teams und seit 2011 CEO der AGON INNOVATION.

Patrick Krauskopf, Jahrgang 1967, ist Rechtsanwalt in Zürich und New York, Harvard-Absolvent, Professor, mehrfacher Verwaltungsratsvorsitzender und Unternehmer der AGON Gruppe.

Weitere Informationen finden Sie unter:
www.agon-innvation.ch

AGON PARTNERS INNOVATION

Seit der Gründung im Jahr 2011 hat sich das Unternehmen **kontinuierlich weiterentwickelt** und bietet heute **hochmoderne Cybersicherheitslösungen** an. AGON PARTNERS Innovation ist führend in der Beratung, Entwicklung und Umsetzung von Cybersicherheitsstrategien sowie im Verkauf von Sicherheitstokens gemäss Schweizer Compliance-Standards. Das Angebot umfasst erstklassige **Swiss Cyber Security** für Kleinbetriebe, Unternehmen, Behörden und Finanzinstitutionen. Dabei setzt das Unternehmen auf eine **enge Zusammenarbeit** mit renommierten Partnern wie AGON Legal, Pexip, Yubico und IBM.

Damit man beim Tanz auf dem Vulkan nicht stolpert

Es ist für Firmen nur eine Frage der Zeit, bis sie von Cyberkriminellen ins Fadenkreuz genommen werden. Darum rüstet SECURIX KMU für den Ernstfall.

Herr Wepfer, Ihr Unternehmen bietet Firmen nicht nur Präventivmassnahmen gegen Cyberangriffe an, sondern steht betroffenen Betrieben auch im Falle einer Attacke als First Responder zur Seite. Richtet sich dieses Angebot auch an KMU?
Es eignet sich sogar perfekt für kleine und mittelgrosse Unternehmen! Denn obschon viele mittelständische Betriebe in der Schweiz fälschlicherweise davon ausgehen, dass sie für Cyberangriffe nicht attraktiv genug sind, stellen KMU mittlerweile das Angriffsziel Nummer eins von Cyberkriminellen dar. Dies, weil sie häufig weniger gut geschützt sind und ihre IT-Infrastruktur nicht selten Sicherheitslücken aufweist. Darüber hinaus verwenden viele Firmen kaum Tools, um sich proaktiv vor Attacken aus dem Web zu schützen oder darüber alarmiert zu werden. Die Kernfrage für KMU lautet dementsprechend nicht mehr, ob sie Opfer von Cyberattacken werden – sondern vielmehr, wann dies eintreten wird. Ich vergleiche das gerne mit dem Tanz auf dem Vulkankrater. Das geht so lange gut, bis der Vulkan ausbricht. Dann ist es entscheidend, einen erfahrenen und versierten Partner wie SECURIX an der Seite zu haben. Das gilt für KMU und Grossbetriebe aller Branchen gleichermassen.

Welche Bedrohungsarten sind denn die gravierendsten für Schweizer Unternehmen?
Es gibt drei wesentliche Szenarien, auf die man achten muss. Da wäre einerseits das Verschlüsseln von Daten zu nennen. Dabei wird einem Unternehmen der Zugang zu seinen Daten verwehrt, wodurch dieses nicht mehr operativ wirken kann. Der operative Betrieb wird also gestört oder sogar komplett unterbrochen – was rasch zu finanziellen Schwierigkeiten führen kann. Ferner sehen wir oft Lösegeldforderungen sowie die Androhung der Veröffentlichung von sensitiven Daten im Darkweb. Letzteres ist besonders für Firmen in hochregulierten Branchen heikel.

Und wie kann SECURIX betroffenen Unternehmen in einer solchen Notsituation helfen?
Ein essenzieller Faktor ist die Reaktionsgeschwindigkeit. Denn je schneller man auf einen Angriff angemessen reagiert, desto geringer fällt der potenzielle Schaden aus. Hier haben wir den enormen Vorteil, dass wir gemeinsam mit unserem internen Cyber-Ökosystem eine rasche und versierte Soforthilfe bei Cybersicherheitsvorfällen anbieten können – und das rund um die Uhr, an jedem Tag des Jahres. Zuerst eruieren wir die Ist-Situation und leiten so schnell wie möglich die passenden Massnahmen in die Wege. Da stehen unter anderem Fragen im Fokus wie: Haben die Angreifer tatsächlich Daten entwendet? Und wissen die Cyberkriminellen eigentlich, wer ihr Opfer ist? Denn Cyberattacken werden oft sehr grossflächig ausgespielt und erst, wenn ein Unternehmen darauf reagiert, weiss die Gegenseite Bescheid, dass sie jemanden erwischt hat. Wir stellen daher auch sicher, dass im Eifer des Gefechts nicht versehentlich die falschen Massnahmen getroffen werden, welche die Situation noch verschlimmern. Zudem koordinieren wir im Ernstfall die Zusammenarbeit mit anderen Stellen, sprich den Behörden und der Polizei. Die Effektivität und Effizienz dieser Dienstleistung lässt sich durch unseren «Emergency Response Retainer» noch zusätzlich erhöhen.

«Ein essenzieller Faktor bei Cyberattacken ist die Reaktionsgeschwindigkeit.»

Gabriel Wepfer
Deputy CEO SECURIX

Wie sieht dieses Angebot konkret aus?
Wir gehen im Rahmen des Retainers mit Kundenunternehmen quasi einen Servicevertrag für Cybervorfälle ein. Retainerkunden können uns rund um die Uhr telefonisch alarmieren und dürfen sich auf eine definierte Reaktionszeit verlassen, alle hierfür notwendigen Details werden im Vorfeld der Zusammenarbeit festgelegt. Zu diesem Zweck findet ein erstes Meeting statt, bei dem wir nicht nur den Geltungsbereich des Emergency Response Retainers definieren, sondern auch die individuellen Bedürfnisse und Möglichkeiten des Kundenbetriebs eruieren. Anschliessend wird für eine definierte Laufzeit ein Vertrag abgeschlossen. Im Rahmen eines gemeinsamen Workshops definieren wir dann die konkreten Prozesse für den Ernstfall, klären Verantwortlichkeiten, stellen einen sauberen Informationsfluss sicher usw. Natürlich geben wir auch für Unternehmen unser Bestes, die nicht Retainerkunden sind – wir können dann aber weder eine festgelegte Reaktionszeit garantieren noch ihre Anliegen priorisiert behandeln.

SECURIX

Erfahren Sie mehr:

Weitere Informationen sowie Kontaktmöglichkeiten finden Sie unter:
www.iam.securix.swiss/sx-incident-response-de

Die Bedrohung durch Cybercrime verändert sich stetig. Wie bleiben Sie am Puls der Zeit?
Wir sind ein Cybersecurity Serviceprovider, der 1996 gegründet wurde und seither seine Expertise konstant erweitert hat. Wir verfügen also über enorme Erfahrung und Knowhow. Zudem wurden wir 2023 Teil der schwedischen Alurity-Gruppe, die europaweit tätig ist. Dieses Netzwerk von Cybersecurityfirmen umfasst mehr als 500 versierte Mitarbeitende, welche die gesamte virtuelle Bedrohungslandschaft abdecken. Davon profitieren natürlich auch unsere Kunden und durch den Wissenstransfer innerhalb der Gruppe sind wir schon heute im Bilde darüber, wie die Angriffsszenarien von morgen aussehen werden. Vor einigen Monaten konnte unser Ökosystem zum Beispiel gemeinsam mit investigativen Journalisten eine chinesische Hackergruppe aufdecken, die rund 75 000 Onlineshops mit gefakten Markenartikeln betrieb.

Gabriel Wepfer, Jahrgang 1992, ist seit 2016 bei SECURIX in verschiedenen Rollen beschäftigt. Seit 2020 in der Rolle CRO und Deputy CEO verantwortet er Sales und Marketing.