CYBERKRIMINALITÄT – Hackerattacken, Ransomware oder Viren: In der Schweiz hat jedes dritte KMU mit Cyberattacken zu kämpfen. Gleichzeitig scheuen sich viele Unternehmen, das Thema anzugehen. Zu Unrecht: Guter Cyberschutz ist umfassend, unkompliziert und bezahlbar – wenn man es richtig angeht.

Ist Cybersecurity ein Luxus?

Vorsorge ist günstiger als Nachsorge – bei Cybercrime zahlt sie sich ganz besonders aus. Bild: zVg

Ein Computervirus legt die Produktion für Wochen lahm – und treibt damit ein Thurgauer Unternehmen in Konkurs. Eine Ransomware-Attacke nimmt die Daten einer bekannten Schweizer Online-Plattform in Geiselhaft – die Lösegeldzahlung befindet sich im sechsstelligen Bereich. Nicht immer sind die Auswirkungen von Cyberattacken so dramatisch. Dennoch sind Schweizer KMU zunehmend davon betroffen. Gemäss dem Allianz Risk Barometer (2020) sind Cyberattacken heute das Risiko Nummer 1 für Schweizer Unternehmen. Jedes dritte KMU hatte schon einmal mit Cybervorfällen zu kämpfen – und diese Zahl steigt jedes Jahr steil an. Die Konsequenzen sind oft kostspielig und schwerwiegend. Trotzdem schützen sich viele Unternehmen schlecht oder gar nicht vor Internet-Kriminalität. Warum? Das hat verschiedene Gründe.

Umfassender Schutz kann ganz einfach sein

Malware, Ransomware oder Darknet: Für viele Unternehmerinnen und Unternehmer sind diese Begriffe weit weg vom Geschäftsalltag. Die Materie ist komplex und die Bedrohung abstrakt: «Manche Kunden sind überrascht, wie einfach es eigentlich ist, sich vor Cyberkriminalität zu schützen», erklärt **John Winter,** Verantwortlicher für Cybersecurity-Lösungen bei Green. Das Schweizer Unternehmen betreut und berät Unternehmen seit über 25 Jahren und ist führend in der IT-Sicherheit. «Aus Angst, dass es zu teuer und zu komplex ist, schieben besonders kleinere Unternehmen das Thema auf die lange Bank. Und das kommt sie dann unter Umständen wirklich teuer zu stehen», so Winter. Oft geht die Cybervorsorge im hektischen Geschäftsalltag auch einfach vergessen – oder die Befürchtungen, Cyberschutz sei kostspielig, stehen entsprechenden Projekten im Weg. Auch wenn wir alle wissen, dass Vorsorge meist günstiger ist als Nachsorge – im Alltag lässt sich dieser Grundsatz alleine nicht immer einfach umsetzen.

Je digitaler, desto angreifbarer

Die zunehmende Digitalisierung hat viele Vorteile für Unternehmen – aber schafft auch neue Bedrohungen. Wenn Personal- oder Kundendaten nur noch digital gespeichert sind, wirkt sich eine entsprechende Attacke tiefgreifend aus. Läuft das Kassensystem digital, muss auch dieses entsprechend geschützt sein. Versicherer, Finanzinstitute oder Gesundheitsdienstleister wie Arztpraxen oder Spitäler sind zudem beliebte Ziele von Cyberkriminellen, denn ihre Daten sind besonders sensibel.

«DER SCHUTZ VOR CYBERBEDROHUNGEN SOLLTE SO SELBSTVERSTÄNDLICH SEIN WIE DIE UNFALLVERSICHERUNG ODER DER EINBRUCHSCHUTZ.»

John Winter, Verantwortlicher für Cybersecurity bei Green

Aber auch kleinere Produktionsbetriebe, Handwerker und die Gastronomie geraten zunehmend ins Visier der Internetkriminalität. Jedes Unternehmen ist angreifbar. Es gibt kaum einen Bereich mehr, der nicht potenziell von Cybercrime betroffen ist. Dabei gilt: Nur wer die Gefahren kennt, kann sie wirksam bekämpfen.

Richtig auf Cyberattacken reagieren

Die digitale Unterwelt ist für die meisten von uns eine unbekannte Grösse. Doch auch wer sich nicht regelmässig im sogenannten Darknet tummelt, sollte die wichtigsten Maschen und ihre Abwehrmechanismen kennen. Grundsätzlich unterscheidet man drei Cybercrime-Typen:

Phishing – Hier «fischen» Cyberkriminelle per SMS, E-Mail oder Telefon nach vertraulichen Daten wie Passwörtern, mit denen sie Zugriff erhalten auf Systeme. Entsprechende Schulungen und Tools können Phishing-Attacken rechtzeitig abfangen.

Malware/Viren – Ein einfacher Klick auf einen infizierten E-Mail-Anhang, und eine Schadsoftware nimmt das ganze IT-System in Beschlag. Welchen Schaden sie anrichtet, hängt von der Art der Software ab. Moderne Antivirus-Programme erkennen schädliche Muster mithilfe künstlicher Intelligenz automatisch.

Ransomware – In der digitalen Form der Erpressung nehmen Cyberkriminelle Daten eines Unternehmens in Besitz, verschlüsseln sie und fordern Lösegeld. Regelmässige, sichere und umfassende Backups können teure Lösegeldzahlungen ersparen.

In drei Schritten zu sicheren Daten

Sichere Daten sind das A und O eines modernen Unternehmens. Ob Virus oder Ransomware: Wer seine Unternehmensdaten regelmässig mit Back-ups sichert, steht im Falle eines Falles besser da. Dabei ist es wichtig, die Daten regelmässig zu sichern, sie langfristig sicher zu halten und auch an die Wiederherstellung zu denken.

1. Daten regelmässig sichern
Daten in regelmässigen Abständen sichern. Je kürzer der Zeitabstand, desto kleiner die Auswirkungen auf den Geschäftsgang. Falls tatsächlich einmal ein Back-up gebraucht wird, hält sich der Datenverlust in Grenzen. Professionelle Back-up-Lösungen automatisieren dies.

2. Daten langfristig sicher halten
Damit Daten in jedem Ereignisfall sicher sind und dies über Jahre hinweg bleiben, sollten sie auf verschiedenen Speichermedien und an unterschiedlichen Speicherorten gehalten werden. Professionelle Back-up-Partner wie Green bieten entsprechende Lösungen: Das Back-up wird automatisch an das Schweizer Green Rechenzentrum übermittelt, bei Bedarf sichert dasselbe Tool auch Daten lokal beim KMU.

3. An die Wiederherstellung denken
Man stelle sich vor: Das Back-up ist vorhanden – aber die Wiederherstellung funktioniert nicht. So etwa, wenn das Back-up unbemerkt vom Cyberangriff ebenfalls betroffen ist. Datensicherheit endet nicht mit dem Back-up. Im Gegenteil: Wirksame Datensicherung alleine reicht nicht aus. Jede Back-up-Lösung ist nur so wertvoll, wie sie die Verfügbarkeit der Daten garantiert. Geeignete Tools validieren jedes Back-up und garantieren so, dass es fehlerfrei wiederhergestellt werden kann.

Ein Unternehmen, das diese Schritte befolgt, kann auf gute Datensicherheit zählen. Doch eines darf nicht vergessen gehen: Die geltenden Datenschutzbestimmungen sind einzuhalten. «Für Schweizer Unternehmen ist es einfacher, wenn sie die Daten in einem Schweizer Rechenzentrum halten», sagt John Winter. «Sie agieren dann unter Schweizer Recht und können auf einen Partner zählen, der nach hiesigen Standards vorgeht.» Ein wichtiger Faktor für die Datensicherheit ist zudem, wie gut Rechenzentren geschützt sind: Gute Rechenzentren verfügen über einen ausgefeilten Zutrittsschutz. Sie berücksichtigen alle Eventualitäten wie Stromunterbrüche, Naturereignisse oder ähnliches in ihren Notfallplänen und treffen Massnahmen, welche die Verfügbarkeit garantieren. Arbeitet man mit einem Partner zusammen, der für Tausende von Kunden in die Datensicherheit investiert, wird auch der Preis attraktiver: «Für einzelne Betriebe ist es schwierig, ein so hohes Sicherheitsniveau zu erreichen», so John Winter. «So ist Sicherheit kein Luxus mehr, sondern selbst für Klein- und Kleinstunternehmen erschwinglich.»

Nur wer die Gefahren kennt, kann richtig reagieren

99 Prozent der Schweizer Unternehmen sind KMU. Das heisst, sie haben weniger als 250 Mitarbeitende. Sie sind das vielbeschworene Rückgrat der Schweizer Wirtschaft – aber auch das anfälligste Glied in der Kette der Datensicherheit. Mangelnde Kenntnis und fehlende Finanzen sind nur scheinbare Hürden, auch digital auf sicheren Beinen zu stehen: In der physischen Welt schützen wir uns wie selbstverständlich vor Eventualitäten wie Bränden, Hochwasser oder Unfällen. Genau so sollten Unternehmen sich vor digitalen Bedrohungen schützen: «Der Schutz vor Cyberbedrohungen sollte zum Unternehmen gehören wie die Unfallversicherung oder der Einbruchschutz», so Winter.

«Cyberkriminelle agieren heute mit Budgets in der Höhe von fünf bis zehn Prozent der globalen Wirtschaftsleistung. Da können einzelne Unternehmen schon lange nicht mehr mithalten.» Die gute Nachricht: Das müssen sie auch nicht. Genau wie Sicherheitsunternehmen oder die Polizei vor physischen Angriffen schützen, bieten externe Anbieter Komplettlösungen, mit denen sich Schweizer Unternehmen umfassend vor den häufigsten digitalen Bedrohungen schützen können.

360° Cyberschutz

Vom E-Mail-Verkehr bis zum Buchhaltungssystem: Ein guter Schutz nimmt alle Bereiche eines Unternehmens in den Blick. Eine ganzheitliche Cybersecurity-Lösung ist verzahnt und hat die verschiedenen Bedrohungen immer im Blick. Dazu braucht es Expertinnen und Experten, die die aktuelle Bedrohungslage verstehen und ständig überwachen. Intelligente Algorithmen prüfen und erkennen Muster innert Sekunden und reagieren sofort auf mögliche Attacken. «Als Finanzunternehmen arbeiten wir mit hochsensiblen Daten», so **Stefan Reist,** Geschäftsleitungsmitglied der Carefinance GmbH in Basel. «Vom Back-up bis zum Virenschutz: Mit der Lösung von Green decken wir alle Sicherheitsaspekte mit einem Tool ab. Und es ist erst noch auf unsere spezifischen Bedürfnisse zugeschnitten.»

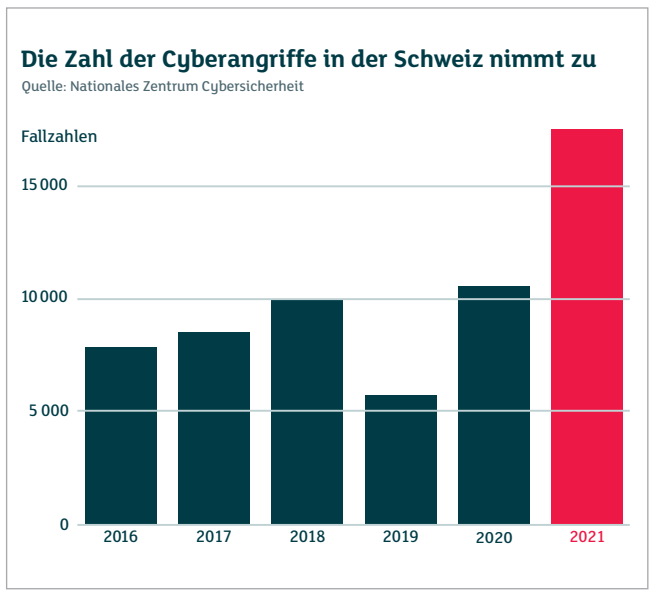
Die etablierte Lösung

Stefan Reist hat sich nach längerer Recherche für die Security-Angebote von Green entschieden. Diese schützen ganzheitlich vor Datenverlust sowie Cyberangriffen – über Daten, Anwendungen und Systeme hinweg. Die Lösung basiert auf einer Cybersecurity-Lösung, die international etabliert und über 180 Länder hinweg im Einsatz ist. Als Datenstandort dienen die Schweizer Rechenzentren von Green – die mehrstufig geschützt sind und von lokalen Experten betrieben werden.

«VOM BACK-UP BIS ZUM VIRENSCHUTZ: MIT EINEM EINZIGEN TOOL DECKEN WIR ALLE SICHERHEITSASPEKTE KOMPLETT AB.»

Stefan Reist, Geschäftsleitungsmitglied der Carefinance GmbH in Basel

Diese Kombination ist einmalig, da sie für KMU umfassende Sicherheit bietet und dennoch erschwinglich ist. Die Zusammenarbeit mit global führenden Partnern sorgt dafür, dass die Cyberabwehr immer auf dem neusten Stand ist. Doch das ist noch nicht alles: «Uns ist wichtig, dass die Tools auch einfach zu bedienen sind», so John Winter. «So halten wir kleinen und mittleren Unternehmen den Rücken frei, damit sie sich wieder voll und ganz auf ihr Kerngeschäft konzentrieren können.»



DONNERSTAG, 27. JANUAR

Frühstücksevent Cybersecurity

Möchten Sie wissen, wie sich Unternehmen vor Cyberbedrohungen einfach und umfassend schützen können? Sie sind herzlich eingeladen zum Cybersecurity Breakfast von Green.
Am **Donnerstag, 27. Januar 2022,** von 8 bis 10 Uhr erfahren Sie, wie Schweizer Unternehmen die Herausforderungen der Cybersicherheit meistern. Diskutieren Sie direkt mit Expertinnen und Experten die wirksamsten Lösungen. Die Plätze sind begrenzt – melden Sie sich noch heute an!

www.green.ch/cybersecurity