RESEARCH AT A GLANCE

ICT-SECURITY: TOPTHEMA IN DEN UNTERNEHMEN

Die ICT-Sicherheit ist nicht nur eine Frage der Technologie

SEPTEMBER 2022

Powered by swisscom

MSM Research AG - Postfach 191 - CH-8201 Schaffhausen
www.msmag.ch - Telefon 052 624 21 21 - info@msmag.ch

INHALT

IMPRESSUM

Quellen / Basis der Studie
Studie "ICT-Security in Schweizer Unternehmen", MSM Research AG, 2022. Im Rahmen der Studie wurden im Sommer 2022 82 Unternehmen in der Schweiz ausführlich zum Thema befragt.

Anmerkung zu den Charts / Resultaten:
Sofern nichts anderes erwähnt ist, waren für die Befragten jeweils Mehrfachantworten möglich.

Autor
Philipp A. Ziegler, CEO, MSM Research AG

Gestaltung / Layout
Corinne Jost, Head of Marketing, MSM Research AG

Publikation
MSM Research AG - Postfach 191 - CH-8201 Schaffhausen - www.msmag.ch
Telefon +41 52 624 21 21 - info@msmag.ch

UNTERNEHMEN STEHEN VOR GROSSEN HERAUSFORDERUNGEN

Die aktuellen globalen Entwicklungen konfrontieren heute viele Unternehmen mit grossen Herausforderungen: Steigende Energiekosten, der Ukrainekrieg, geopolitische Konflikte, der Chipmangel, Lieferkettenprobleme, der Klimawandel und Inflationssorgen schaffen nach dem Ende der Pandemiemassnahmen erneut Planungsunsicherheiten.

Auch wenn die Schweizer Unternehmen im Vergleich zum Pandemiebeginn Anfang 2020 heute deutlich robuster und proaktiver aufgestellt sind, werden geplante Investitionen und Projekte derzeit wieder zögerlicher und vorsichtiger angegangen. Der Gegenwind auf der Planungsfront dürfte weiter zunehmen. Abseits von wirtschaftlichen Herausforderungen stehen aus Sicht der im Rahmen unserer neuen Studie befragten Unternehmen die Themen ICT-Sicherheit und Business Continuity Management ganz oben auf dem Sorgenbarometer.

«Die ICT sicherzustellen ist zurzeit eine der grössten Herausforderungen im Unternehmen»

So stufen vier von fünf befragten Unternehmen die Sicherheitsgefährdung im ICT-Bereich, resp. die zunehmende Bedrohung durch Cyberattacken/ Cyberkriminalität als aktuelles Topthema ein. Dies sowohl mit Blick auf die steigende Anzahl als auch mittlerweile hohe Professionalität der Angriffe.

Allein in der Woche 30 des laufenden Jahres wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) 684 neue Cybervorfälle gemeldet. Und dies nicht nur in den Top-Kategorien Betrug, Ransomware und Phishing, sondern auch in einer mittlerweile 18 Kategorien umfassenden Liste an Cyberbedrohungen.

Welche allgemeinen Themen beschäftigen Sie im Unternehmen zurzeit am meisten?

Die Businessprozesse und die Wertschöpfung sichern

Die aktuell hohe Bedeutung des Themas ICT-Sicherheit wird auch durch die Anzahl der Projekte sichtbar: In mehr als 80% der Unternehmen steht das Thema Security an erster Stelle in den ICT-Abteilungen.

Dies ist ein deutliches Zeichen für ein starkes Bewusstsein und die klare Ausrichtung der Projekt-Arbeiten mit Blick auf einen sicheren Betrieb und eine hohe Verfügbarkeit der Prozesse und Anwendungen.

Aber auch in den Fachabteilungen sind Sicherheitsfragen und das etwas weitergefasste Thema des Risk Management für knapp die Hälfte der Unternehmen an oberster Stelle ihrer Agenda anzutreffen.

In das Thema Risiko Management der Businessabteilungen mit einbezogen werden dabei nicht nur rein rechtliche Risiken mit Blick auf den Umgang mit Daten, sondern auch Fragen um die Sicherstellung des Weiterbetriebes und der Hochverfügbarkeit der ICT-Infrastruktur und Anwendungen im Katastrophenfall.

«Das Business ist auf einen sicheren und hochverfügbaren ICT-Betrieb angewiesen»

Die 3 Hot Topics aus dem Business und ICT-Umfeld

(44% der Projekte ICT-getrieben, 56% Business-getrieben, Total 316 Projekte)

Projekte aus den Business-Bereichen

48% **Datenschutz**
(Risk Management, GDPR, DSGVO)

40% **ERP**
(Enterprise Ressource Planning)

37% **Workplace**
Mobile Lösungen, Remote & Home Office, UCC/Video-Lösungen

Projekte aus der ICT

85% **ICT-Security**

39% **ICT-Betrieb, Cloud & hybride Architekturen**

34% **Multi-Cloud**

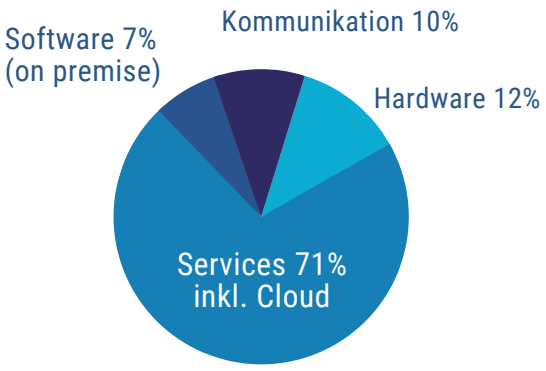
DIE ICT-AUSGABEN UND DER HOHE STELLENWERT DER SECURITY

Die Auswirkungen der aktuellen Krisen schlagen auch auf die wirtschaftliche Situation und Entwicklung in der Schweiz durch. Gemäss der KOF (Konjunkturforschungsstelle der ETH) Frühjahrsprognose 2022 wird die Schweizer Wirtschaft in diesem Jahr im günstigen Szenario um knapp 3% wachsen. Und die EU hat ihre Wachstumsprognose mittlerweile auf 2.7% gesenkt. Weitere Korrekturen sind kaum auszuschließen.

Trotz der angespannten wirtschaftlichen Situation und eher unsicheren Aussichten planen die Schweizer Unternehmen auch im laufenden Jahr ihre Budgets aufzustocken.

Wir rechnen für 2022 mit einem Wachstum der ICT-Spendings (B2B) im günstigen Fall von 4.5%. Damit würden die Ausgaben erstmals auf über 20 Milliarden Franken steigen, was einem Volumen von mehr als 84 Millionen Franken an Projektausgaben und Aufträgen pro Arbeitstag entspricht.

Der Löwenanteil der ICT-Ausgaben (B2B) entfällt heute auf die ICT-Services, also den Dienstleistungssektor im ICT-Markt. Im laufenden Jahr 2022 rechnen wir auf der Basis unserer aktuellen Frühjahrsprognose mit einem Anteil der Services am gesamten ICT-Markt von 71%. Damit werden deutlich mehr als zwei von drei Franken der ICT-Spendings an Dienstleister und Provider überwiesen.



Total ICT-Ausgaben 2022: 20'064 Mio CHF

Wachstum 2021/2022: +4.5%

Projektausgaben von 84 Mio CHF / Tag

«Der ICT-Markt ist ein Dienstleistungsmarkt»

Ein Trend, der sich weiter fortsetzt, die Schere zwischen Services und übrigen Ausgaben wird sich weiter zugunsten der Dienstleistungen öffnen. Dies auch mit Blick auf die vermehrte Verschiebung der Ausgaben im ICT-Security Bereich hin zu externen Service-Anbietern.

DIE AUSGABEN FÜR ICT-SECURITY WERDEN MASSIV AUFGESTOCKT

Schweizer Unternehmen geben viel Geld für die Sicherheit und Hochverfügbarkeit der ICT aus. So wurden 2021 2.7 Milliarden Schweizer Franken für Appliances (HW), Lösungen (SW) und Services ausgegeben. Und auch im laufenden Jahr erwarten die Unternehmen mehrheitlich eine Erhöhung der externen Ausgaben für die ICT-Sicherheit. Wir gehen von einem Anstieg der ICT-Security Ausgaben in der Schweiz von 8.3% aus.

Die höchsten Zuwachsraten erfahren aktuell die Ausgaben für Services durch die steigende Inanspruchnahme der Leistungen externer Dienstleister. So rechnen wir für das laufende Jahr mit einer Aufstockung der entsprechenden Gelder für externe Services um knappe 10%.

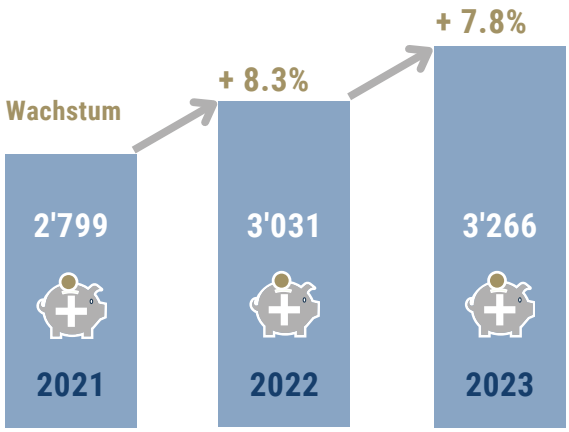
Mittlerweile fliessen mehr als 12% der ICT-Ausgaben in die Sicherheit und Hochverfügbarkeit der ICT.

Ein eigenes Budget für die ICT-Security

Aber auch für die ICT-Sicherheit stehen nicht immer Gelder ohne Ende zur Verfügung, erschwerend in manchen Unternehmen kommt hinzu, dass die geplanten Budgets, Ausgaben und Projekte oft sogenannten "Moving Budgets" zum Opfer fallen oder verschoben werden. So können kurzfristig andere Vorhaben aus Fachabteilungen vorgezogen werden oder Ausgaben für die Modernisierung und den Ausbau der Infrastruktur eine höhere Priorität bei der Umsetzung erhalten.

Ein Weg aus diesem Dilemma der Abhängigkeit könnte die Herauslösung des Security-Budgets aus dem ICT-Budget sein, um mit einem unabhängig geführten Geldtopf die Ausgaben für die Sicherheit isoliert und autonom festzulegen und zu managen.

ICT-Security Ausgaben in der Schweiz	**2021** in Mio CHF
Security Lösungen (on premise)	949
Security Appliances	362
Security Services	1'488
Total ICT-Security Markt	**2'799**



DIE BEDROHUNGSLAGE UND DER FAKTOR MENSCH

Im Jahr 2021 wurden von der Polizei in der Schweiz 30'351 Straftaten mit einer digitalen Komponente registriert, was einem Durchschnitt von 83 digitalen Straftaten pro Tag entspricht. Diese erhöhten sich von 24'398 im 2020 um 24%. Nahezu 88% betrafen die «Cyber-Wirtschaftskriminalität». (Quelle: Polizeiliche Kriminalstatistik (PKS), Bundesamt für Statistik).

Cyber Crime und Attacken auf Unternehmen können nicht nur grossen finanziellen Schaden anrichten und Imageschäden verursachen, sondern auch für das Management, den VR oder Inhaber Konsequenzen nach sich ziehen.

«Der Faktor Mensch ist die grösste Hürde für die Einhaltung der ICT-Sicherheit»

Unsere neue Studie hat deutlich gemacht, dass die derzeit bedeutendste Bedrohung für über 65% der Unternehmen die fehlende Awareness und Sensibilisierung der Mitarbeitenden ist. Die grösste Hürde bei der Umsetzung und Einhaltung entsprechender Sicherheitsvorgaben ist also der Mensch.

So gaben die befragten Unternehmen zu Protokoll, dass die fehlende Zeit, sich um Securitybelange zu kümmern sowie das mangelnde Bewusstsein um die Risiken und Folgen eines Fehlverhaltens und letztlich der Mangel an Kompetenz und entsprechender Fachkräfte im Unternehmen, die Sicherheitsdispositive am meisten gefährden.

Welches sind in Ihrem Unternehmen die wichtigsten Hemmfaktoren und Hürden zur Umsetzung und Einhaltung der ICT-Sicherheit?

52%

Zu wenig Zeit und Kapazität / Chronische Überlastung Mitarbeitende

34%

Mangelndes Security Know how / fehlende Fachkräfte

24%

Mangelnde Unterstützung durch das Management

Gerade auch der Trend zur Hybridisierung der Arbeitsplatzwelt und Verlagerung der Arbeit in Homeoffices fordert die Security Verantwortlichen und die Mitarbeitenden mit Blick auf Sicherheitsaspekte verstärkt heraus.

«Die Digitalisierung, der hybride Workplace sowie die Cloud schaffen neue Angriffsflächen»

Zudem schafft die starke Verbreitung und Nutzung von Cloudservices sowie die Vielzahl an datensammelnden Devices im Zuge von IoT-Projekten weitere Angriffsflächen für Cyberattacken.

Aus welchen Quellen und Bereichen geht aus Ihrer Sicht aktuell die grösste Sicherheits-Bedrohung aus?

65%

Mangelnde Awareness bei den Mitarbeitenden

57%

Böswillige Attacken durch Hacker

DER UMGANG MIT DEN GRÖSSTEN SICHERHEITSRISIKEN

Eine der grossen Gefahrenquellen und Sicherheitsrisiken aus Sicht der Unternehmen stellt der Umgang der Mitarbeitenden mit E-Mails oder auch mit Messages aus sozialen Medien dar. So wird das bewusste oder auch unbewusste Öffnen unsicherer, unbekannter Links oder auch das Anklicken infizierter Attachments aus sogenannten "Phishing Mails" als grösste Gefahrenquelle genannt.

Grösstes Risiko für die Unternehmen: Umgang mit E-Mails (z.B. Phishing, Anklicken von unsicheren Links, Öffnen infizierter Attachements)

Zu den weiteren grossen Gefahrenquellen zählen aber auch der Umgang mit dem Internet. Durch den Besuch von manipulierten Webseiten oder Eingeben von Daten auf unsicheren Webseiten können so Trojaner oder Ransomware auf den Rechner des Anwenders eingeschleust werden.

Mit solchen Manipulationen und Angriffen durch Cyberkriminelle werden immer die Ziele verfolgt, beim Anwender unrechtmässig persönliche Daten oder geistiges Eigentum (Spionage) abzugreifen, Zugang zu Finanzkonti zu erhalten, Erpressergeld zu verlangen oder anderweitig Schaden anzurichten.

«Ransomware, Phishing Mails und generell der Umgang mit dem Internet sind die grössten Gefahrenquellen»

Gerade die Folgen der Pandemie, wie die Verlagerung der Arbeitsplätze ins Home Office, hat vielen Unternehmen mit Blick auf die Sicherheit die Augen auf vorhandene Schwächen und Sicherheitslücken geöffnet.

Sich aber alleine der neuen Risiken bewusst zu werden, wird nicht reichen, um einen möglichst umfassenden Schutz zu gewährleisten. Zur Vorbeugung gehören sowohl technische und organisatorische Massnahmen als auch eine proaktive und sicherheitsbewusste Mitarbeit der Mitarbeitenden.

Zu den Top drei technischen und organisatorischen Massnahmen, Risiken zu minimieren, zählen die regelmässige Sensibilisierung und Schulung der Mitarbeitenden über den sicheren Gebrauch von E-Mail und Internet, beschränkte Nutzerrechte und Access Management (z.B. persönliche Logins) sowie Multi-Faktor-Logins.

Zur lückenlosen Umsetzung der Sicherheitsdispositive und Sicherstellung der Hochverfügbarkeit der ICT-Infrastruktur verlangt es aber nach mehr als einem umfassenden Technologie-Einsatz. Man würde einer falschen Logik unterliegen, davon auszugehen, dass alleine dadurch eine höhere Sicherheit erlangt werden kann.

ICT-Sicherheit ist nicht ausschliesslich eine finanzielle oder technologische Frage, sondern eine der gelebten Kultur und Disziplin aller Mitarbeitenden im Unternehmen.

Wie gehen Sie mit Sicherheitsrisiken im Unternehmen um, welche Massnahmen treffen Sie?

73%

Regelmässige Sensibilisierung der Mitarbeitenden über den sicheren Gebrauch von E-Mail und Internet

67%

Beschränkte Nutzerrechte / Access Management (z.B. persönliche Logins)

56%

Multi-Faktor-Logins

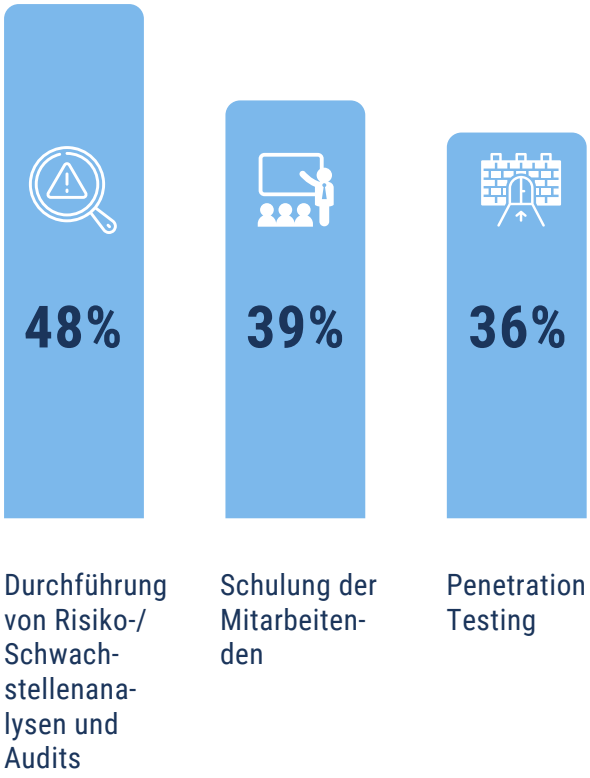
DER BIG SHIFT – UNTERSTÜTZUNG DURCH EXTERNE PROVIDER

Um der steigenden Anzahl an Cyberattacken entsprechend begegnen zu können, arbeiten heute viele Unternehmen im Bereich der ICT-Security mit externen Dienstleistern und Providern zusammen. Zusätzlich bringt die in hohem Tempo fortschreitende Entwicklung neuer Technologien viele Unternehmen an ihre Grenzen.

«Externe Unterstützung ist angesagt»

Heue werden die Angriffe immer komplexer und die Schutzmaßnahmen können durch Angreifer umgangen werden. Eine Attacke kann so für mehrere Tage, Wochen und sogar Monate unentdeckt bleiben. Daher ist es notwendig, moderne Erkennungssysteme einzurichten, um einen Angriff so schnell wie möglich zu erkennen und abzuwehren. Für eine umfassende Vorbereitung auf entsprechende Vorfälle (Incident Response) fehlen in den Unternehmen aber oftmals die Fachkräfte mit spezifischer Expertise. Hier bieten erfahrene und spezialisierte Dienstleister mit ihrem Know-how professionelle Unterstützung.

In welchen Bereichen nehmen Sie heute Dienstleistungen eines externen ICT-Security-Serviceanbieters in Anspruch?



So nehmen bereits heute vier von fünf Unternehmen Services externer Dienstleister in Anspruch oder planen dies in den kommenden zwei Jahren zu tun. Vorab sind dies Services in den Bereichen Risiko-/Schwachstellenanalysen sowie Audits, Schulung der Mitarbeitenden und Penetration Testing.

Die weiter zunehmende Cyberkriminalität und Komplexität der Angriffe, die fehlende oder nicht adäquate Security Kompetenz (inkl. Threat Intelligence Wissen) und die steigende Nutzung von Multi-Cloud Services sind die wichtigsten Keydrivers der Unternehmen, externe Managed Security Services (MSS) in Anspruch zu nehmen.

Managed Security Services umfassen für Teil- oder ganze Bereiche der ICT-Infrastruktur und Netze eine systematische und kontinuierliche sicherheitstechnische Überwachung auf Schwachstellen, Lücken und Attacken. Entsprechende Managed Security Service Provider (MSSP) sind in der Lage, rasch, kompetent und agil auf sich ändernde Bedrohungslagen zu reagieren - und dies zu transparenten, planbaren Kosten und klar definierten Services.

«Managed Security Service Provider (MSSP) sind in der Lage, rasch, kompetent und agil auf sich ändernde Bedrohungslagen zu reagieren»

Über 64% der befragten Unternehmen planen, aufgrund der zunehmenden Cyber-Bedrohungen und steigenden Anforderungen an die Sicherheit künftig verstärkt mit externen Dienstleistern und MSSP zusammenzuarbeiten.

Und über 20% nehmen aufgrund der aktuellen Risikolage und fehlenden internen Ressourcen die Evaluierung externer Service Anbieter beschleunigt in Angriff.

Der im Bereich des ICT-Betriebes bereits seit geraumer Zeit zu beobachtende Paradigmenwechsel (von intern zu extern) oder Big Shift nimmt auch im Bereich der Sicherheit weiter Fahrt auf. Die Verlagerung von bislang intern selbst erbrachten Aufgaben, Arbeiten und Dienste an externe Provider hat auch im Bereich der ICT-Sicherheit deutlich an Fahrt aufgenommen.

Welches sind die Keydriver, externe Managed Security Services (MSS) in Anspruch zu nehmen?

93%

Weiter zunehmende Cyberkriminalität / Komplexität der Angriffe

41%

Fehlende oder nicht adäquate Security Kompetenz (inkl. Threat Intelligence Wissen)

18%

Nutzung von Multi-Cloud Services, Erhöhung Angriffsflächen

SUMMARY - WICHTIGE ERKENNTNISSE

- Cyber Crime und Attacken auf Unternehmen können nicht nur grossen finanziellen Schaden anrichten und Imageschäden verursachen, sondern auch für das Management, den VR oder Inhaber Konsequenzen nach sich ziehen.

- Für über 65% der Unternehmen ist die derzeit bedeutendste Bedrohung die fehlende Awareness der Mitarbeitenden.

- Eine der grossen Gefahrenquellen stellt der Umgang der Mitarbeitenden mit E-Mails oder auch mit Messages aus sozialen Medien dar.

- Zu den Top drei technischen und organisatorischen Massnahmen, Risiken zu minimieren, zählen die regelmässige Sensibilisierung und Schulung der Mitarbeitenden, beschränkte Nutzerrechte und Access Management sowie Multi-Faktor-Logins.

- Trotz der eher unsicheren Aussichten planen Schweizer Unternehmen die Aufstockung ihrer Budgets im 2022; wir rechnen mit einem Wachstum der ICT-Spendings (B2B) von 4.5%.

- Die höchsten Zuwachsraten im Bereich der ICT-Security erfahren aktuell die Ausgaben für Services durch die steigende Inanspruchnahme der Leistungen externer Dienstleister.

- Für Sicherheit und Hochverfügbarkeit der ICT haben Schweizer Unternehmen 2021 2.7 Milliarden Schweizer Franken für Appliances (HW), Lösungen (SW) und Services ausgegeben. Im 2022 erwarten die Unternehmen mehrheitlich eine Erhöhung der externen Ausgaben für die ICT-Sicherheit. Wir gehen von einem Anstieg von 8.3% aus.

- Um der steigenden Komplexität und zunehmenden Anzahl an Cyberattacken begegnen zu können, arbeiten heute viele Unternehmen im Bereich der ICT-Security mit externen Dienstleistern zusammen. Heute nehmen vier von fünf Unternehmen Services externer Dienstleister in Anspruch oder planen dies in den kommenden zwei Jahren zu tun.

- Die weiter zunehmende Cyberkriminalität und Komplexität der Angriffe, die fehlende oder nicht adäquate Security Kompetenz (inkl. Threat Intelligence Wissen) und die steigende Nutzung von Multi-Cloud Services sind die wichtigsten Keydrivers der Unternehmen, externe Managed Security Services (MSS) in Anspruch zu nehmen.

FAZIT

Kein Unternehmen ist vor Cyberangriffen gefeit. Auch wenn die Pandemie und ihre Folgen das Bewusstsein um Sicherheits-Risiken und Schwachstellen gesteigert hat, entsprechende Konzepte werden noch nicht überall konsequent durchgesetzt. Es darf nicht sein, dass erst im Falle eines Ereignisses reagiert und Massnahmen aufgesetzt werden. Solche Flickenteppiche sind keine adäquate Antwort.

ICT-Security darf auch nicht zur reinen Kostenfrage verkommen und entsprechend geplante Budgets sollten nicht anderen Projekt-Prioritäten zum Opfer fallen.

Ein Weg aus diesem Dilemma der Abhängigkeit könnte die Herauslösung des Security-Budgets aus dem ICT-Budget sein, um mit einem unabhängig geführten Geldtopf die Ausgaben für die Sicherheit isoliert und autonom festzulegen und zu managen.

ICT-Sicherheit ist aber nicht ausschliesslich eine finanzielle oder technologische Frage, sondern eine der gelebten Kultur und Disziplin aller Mitarbeitenden im Unternehmen.

Eine alles umfassende und möglichst flächendeckende Sicherheit beinhaltet nicht nur die Sicht nach aussen und Massnahmen aufgrund aktueller Bedrohungslagen und Risiken, sondern bedarf auch Vorkehrungen auf der Basis einer kritischen Sicht auf die Organisation und den Faktor Mensch.

Denn das verantwortungsvolle, sicherheitsbewusste Verhalten aller Mitarbeitenden, der sensible Umgang mit Daten ist letztlich die wirkungsvollste Verteidigungslinie und «Firewall» im Kampf gegen Cyber-Attacken und Ausfälle der ICT.

WIE KÖNNEN UNTERNEHMEN ERFOLGREICH RANSOMWARE-ATTACKEN VERHINDERN?

«Jedes Unternehmen benötigt wirksame Massnahmen gegen Ransomware»

Stephan Rickauer leitet bei Swisscom den CSIRT-Service und CSIRT Rapid Response für Geschäftskunden.

Weshalb ist Ransomware eine so grosse Bedrohung für Unternehmen?

Stephan Rickauer: Wahrscheinlich, weil die Bedrohung so konkret und umfassend ist. Ich kenne keinen CEO, der mir bei einem Rapid Response Case entspannt mitgeteilt hätte: «Herr Rickauer, keine Eile, wir können auch ohne IT unser Kerngeschäft verfolgen». Ohne IT verkauft man heute keine Gipfeli mehr. Das macht jede Firma erpressbar.

Hinzu kommt, dass viele Firmen unzureichend auf einen Ransomware-Angriff vorbereitet sind. Das lässt sich gut an den fast täglichen Medienberichten ablesen. Meistens wird nicht mal das Allernötigste unternommen. Ein Beispiel: Eine Firma hat ein System, das zwei Jahre lang nicht gepatcht wurde, direkt ans Internet angebunden, um «kurzfristig» ein Problem zu lösen. Die Abschaltung ging vergessen, der Server wurde kontaminiert und diente als Einfallstor für die firmenweite Verschlüsselung. Die Folgen waren ein Schaden von über 100'000 Franken und mehrere Tage Downtime.

Was sind die aktuellen Entwicklungen bei Ransomware?

Wir sehen eine zunehmende Professionalisierung der Angriffe. Die einzelnen Jobs sind aufgeteilt. Es gibt Access Broker, die nur Zugänge verkaufen. Und es gibt Malware as a Service, deren Entwickler sogar SLA für die Angreifer anbieten. Wir haben es hier mit einem Industriezweig zu tun, nicht mit arbeitslosen Kreativen.

Die gute Nachricht ist, dass die Entwicklung auch auf der Verteidigerseite nicht stehengeblieben ist. Was früher der Virenscanner war, heisst heute «Endpoint Protection» und ist für uns im Incident-Response-Team immer das erste, was wir im Notfall ausrollen. Auch ist das Thema Security wesentlich präsenter als noch vor sechs oder acht Jahren. Es ist ein neuer, grosser Industriezweig auch auf der Verteidigerseite entstanden. Kritische Infrastrukturbetreiber, wie auch wir bei Swisscom, investieren heute wesentlich mehr in Cyberabwehrmassnahmen.

Was müssten denn Unternehmen machen, um den Schutz zu verbessern?

Stephan Rickauer: Die Geschäftsleitung ist dafür verantwortlich, die Überlebensfähigkeit des Unternehmens sicherzustellen. Dazu gehört heute der Schutz vor Ransomware wie der Sicherheitsgurt im Auto. Aber das Thema schreckt ab, ist komplex und der Markt unübersichtlich.

Ich rate daher Unternehmen, eine Sicherheitsüberprüfung extern zu beauftragen und dann risikobasiert und schrittweise vorzugehen. Das ist bezahlbar und muss auf die Agenda der Entscheidungsträger.

Die gute Nachricht: Es gibt viele Anbieter von Managed Security Services, die auch für KMU erschwinglich sind. Nicht jede Firma muss eigene Cybersecurity-Spezialisten ausbilden. Aber die Gefahren müssen bekannt und die Massnahmen dagegen wirksam sein.

swisscom

Über Swisscom Business Customers

Der Geschäftsbereich Business Customers von Swisscom ist einer der grössten, integrierten ICT-Anbieter für Grosskunden und KMU in der Schweiz. Die Kernkompetenzen von Swisscom Business Customers sind integrierte Kommunikationslösungen, IT-Infrastruktur, IT-Security und Cloud Services, Workplace-Lösungen, SAP Services, IoT sowie umfassende Outsourcing-Leistungen für die Finanzindustrie und Health Care. Swisscom Business Customers betreut mit rund 5'000 Mitarbeitenden gut 2'500 Grosskunden und rund 250'000 KMU.

Security bei Swisscom Business Customers

Swisscom Business Customers ist gemäss unabhängigen Studien die führende Anbieterin von Security Services in der Schweiz. Unsere Security-Fachleute setzen sich Tag für Tag für die Informationssicherheit von Schweizer Unternehmen ein. Swisscom bietet Kunden ein grosses Angebot an dedizierten und bewährten Managed Security Services, u.a. ein 7×24 Security Operation Center mit Zugriff auf Security-Spezialisten.

Weitere Informationen zu den Swisscom Managed-Security-Produkten finden Sie unter https://www.swisscom.ch/security

COPYRIGHT UND NUTZUNGSBESTIMMUNGEN

Dieses Whitepaper wurde von MSM Research AG, powered by Swisscom, zur Weitergabe an ihre Kunden erstellt.

Die darin enthaltenen Informationen und Angaben wurden gewissenhaft und mit grösstmöglicher Sorgfalt und Korrektheit ermittelt. Annahmen und Schätzungen sind unumgänglich, sie entsprechen unserem aktuellen Wissensstand. Für deren Vollständigkeit und Richtigkeit kann jedoch keine Garantie übernommen werden.