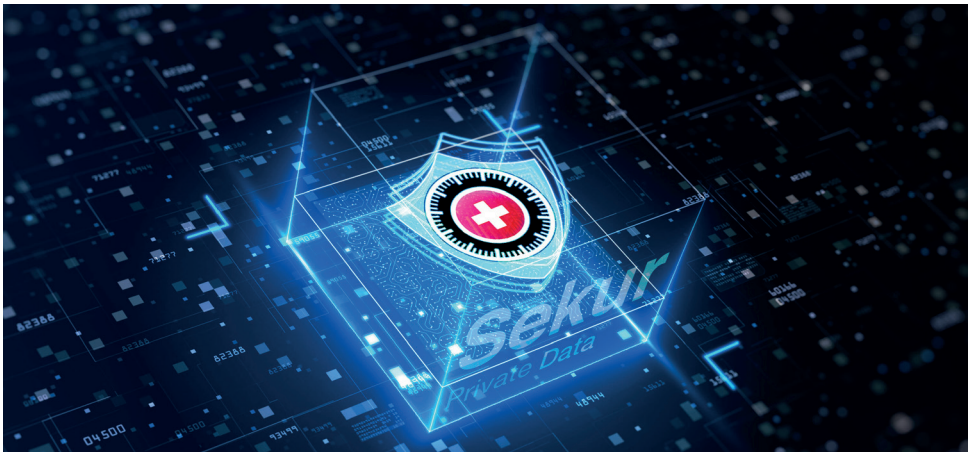
Rockstone Research

22. September 2023

Report #1

Cybersecurity



Die Schweizer Festung der digitalen Sicherheit

WÄCHTER DES CYBERSPACE:

WIE SICH JEDER GEGEN CYBERKRIMINALITÄT WEHREN UND DIE PRIVATSPHÄRE OHNE BIG-TECH-GIGANTEN SCHÜTZEN KANN

In den letzten Jahren hat die digitale Welt einen dramatischen und alarmierenden Anstieg von Cyberangriffen und Datenschutzverletzungen erlebt. Die Ausbreitung dieser Angriffe und Datenpannen hat Regierungen, Unternehmen und Privatpersonen gleichermaßen erschüttert. Da die Weltbevölkerung immer stärker vernetzt und von der digitalen Technologie abhängig ist, war der Bedarf an robusten Sicherheitsprodukten noch nie so groß wie heute. Regierungen, Unternehmen und Privatpersonen müssen proaktive Maßnahmen ergreifen, um die wachsende Bedrohung durch Cyberkriminalität einzudämmen und dem zunehmenden Bedürfnis nach Datenschutz Rechnung zu tragen. Indem wir die sich entwickelnde Natur von Cyberbedrohungen erkennen und präventive Schritte zu ihrer Abwehr unternehmen, können wir hoffen, unsere digitale Zukunft zu sichern und die Grundlagen unserer vernetzten Welt zu schützen.

In einer Zeit, in der die digitale Welt ein integraler Bestandteil unseres täglichen Lebens ist, kann die Bedeutung von Sicherheit und Datenschutz gar nicht hoch genug eingeschätzt werden. Angesichts der zunehmenden Komplexität von Cyber-Bedrohungen und der immer größer werdenden Angriffsfläche befinden sich Unternehmen, die Cybersicherheitsprodukte verkaufen, in einer Position von großer Relevanz und Chance.

Laut McKinsey beläuft sich der weltweit adressierbare Markt für Cybersicherheitsprodukte auf schwindelerregende $2 Billionen USD, jedoch haben die Produktanbieter bisher nur 10% dieses expansiven Marktes erschlossen. Diese riesige Lücke stellt eine beispiellose Gelegenheit für Unternehmen dar, ihre Produktportfolios zu erweitern, Innovationen zu fördern und das immense Wachstumspotenzial innerhalb der Cybersicherheitsbranche zu nutzen.

Sekur Private Data Ltd. hebt sich von anderen Unternehmen im Bereich Cybersicherheit und Datenschutz durch sein einzigartiges Produktportfolio und einen stetig wachsenden Kundenstamm ab. Mit innovativen Lösungen, die auf die sich entwickelnden digitalen Bedrohungen und die Belange des Datenschutzes zugeschnitten sind, hat sich Sekur einen exzellenten Ruf für den Schutz sensibler Informationen erworben und positioniert das Unternehmen und seine Aktionäre für vielversprechende Wachstumsperspektiven in der sich ständig weiterentwickelnden Landschaft der Cybersicherheit.

Unternehmensdetails

Sekur® Private Data

Sekur Private Data Ltd.
Suite 5600 –100 King Street West
Toronto, ON, M5X 1C9 Canada
Phone: +1 416 644 8690
Email: corporate@sekurprivatedata.com
www.sekurprivatedata.com

ISIN: CA2006977045

Aktien im Markt: 119.632.941

Chart Kanada (CSE)

Kanada-Symbol (CSE): SKUR
Aktueller Kurs: $0,20 CAD (21.09.2023)
Marktkapitalisierung: $24 Mio. CAD

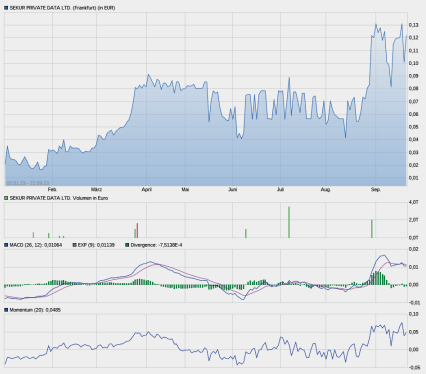


Chart Deutschland (Frankfurt)

Deutschland-Ticker / WKN: GDT0/ A3DKJ0
Aktueller Kurs: €0,122 EUR (21.09.2023)
Marktkapitalisierung: €15 Mio. EUR

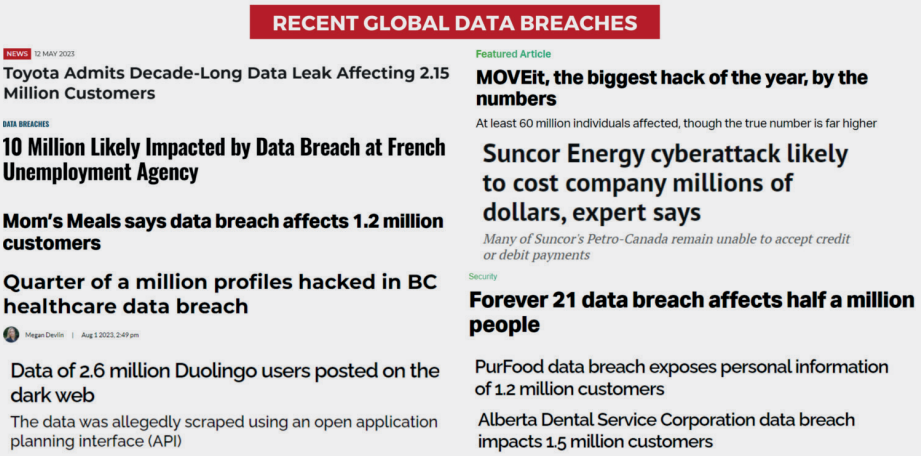
Alle $-Zahlen in CAD, sofern nicht anders angegeben.

Die Cybersicherheitsbranche hat in den letzten Jahren eine Welle von Fusionen und Übernahmen (M&A) erlebt. Etablierte Technologieunternehmen und Private-Equity-Firmen haben den immensen Wert von Sicherheits- und Datenschutzlösungen erkannt und investieren aktiv in Unternehmen, die in diesem Markt tätig sind, oder übernehmen sie. Dieser Zufluss von Kapital und Fachwissen bestätigt die glänzende Zukunft dieser florierenden Branche.

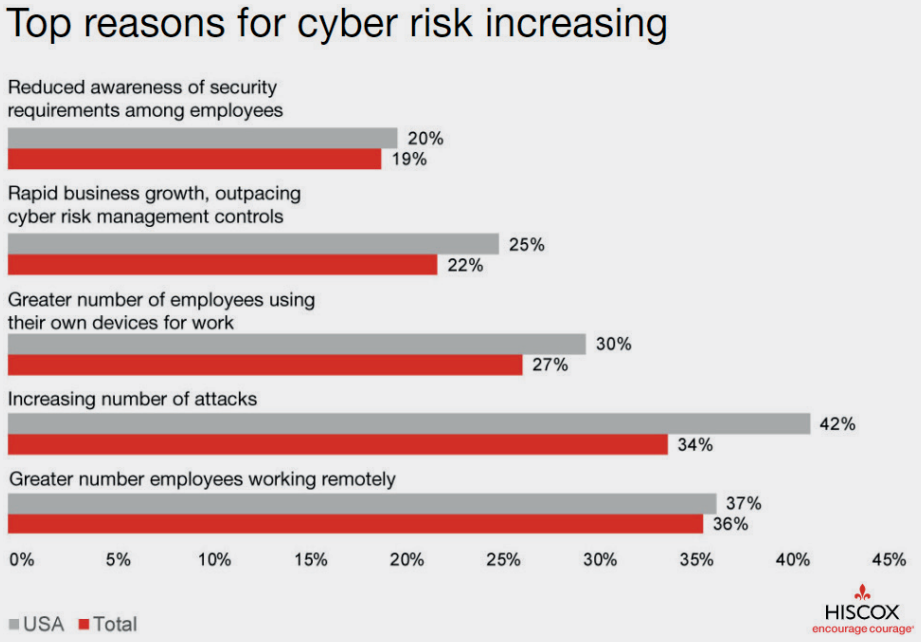
Der erste und vielleicht überzeugendste Grund für die glänzende Zukunft der Cybersicherheitsunternehmen ist die eskalierende Cyberbedrohungslandschaft. Cyberangriffe sind raffinierter, vielfältiger und häufiger geworden als je zuvor. Hacker entwickeln ständig neue Techniken, um in Netzwerke einzudringen, Daten zu stehlen und den Betrieb zu stören. Solange Cyberbedrohungen fortbestehen und sich weiterentwickeln, wird es eine ständige Nachfrage nach innovativen Lösungen für Cybersicherheit und Datenschutz geben.

Die Menschen sind sich der Bedeutung der Cybersicherheit für ihr privates und berufliches Leben zunehmend bewusst. Dieses gesteigerte Bewusstsein treibt die Nachfrage nach Cybersicherheitsprodukten an. In dem Maße, wie Regierungen und Unternehmen sicherheitsbewusster werden, werden Unternehmen, die Cybersicherheitsprodukte verkaufen, einen wachsenden Markt für ihre Angebote finden.

Mit kontinuierlicher Innovation, Anpassung an neue Bedrohungen und dem Engagement für den Schutz digitaler Systeme wird die Cybersicherheitsbranche auch weiterhin eine wichtige Rolle beim Schutz unserer vernetzten Welt spielen.



Die obige Zusammenstellung der jüngsten weltweiten Datenschutzverletzungen stammt aus dem Artikel „Sekur: Safeguarding your digital world" (15. September 2023). Kürzlich wurden zwei Hotels in Las Vegas Opfer von Cyberangriffen und erschütterten damit die öffentliche Wahrnehmung, dass die Sicherheit von Kasinos einen Aufwand auf dem Niveau von „Ocean 11" erfordert, um sie zu überwinden. Sowohl MGM Resorts als auch Caesars Entertainment haben die jüngsten Angriffe bestätigt, die zu einer Reihe von Störungen geführt haben, darunter die Unzugänglichkeit von Türen in den Casinos und Hotels des Unternehmens, nicht funktionierende Spielautomaten und Geldautomaten, nicht funktionierende Aufzüge und langwierige Verzögerungen beim Check-in der Gäste. Caesars hat bereits etwa die Hälfte eines Lösegelds in Höhe von $30 Mio. USD gezahlt, das Hacker nach einem Cyberangriff im Spätsommer dieses Jahres gefordert hatten.



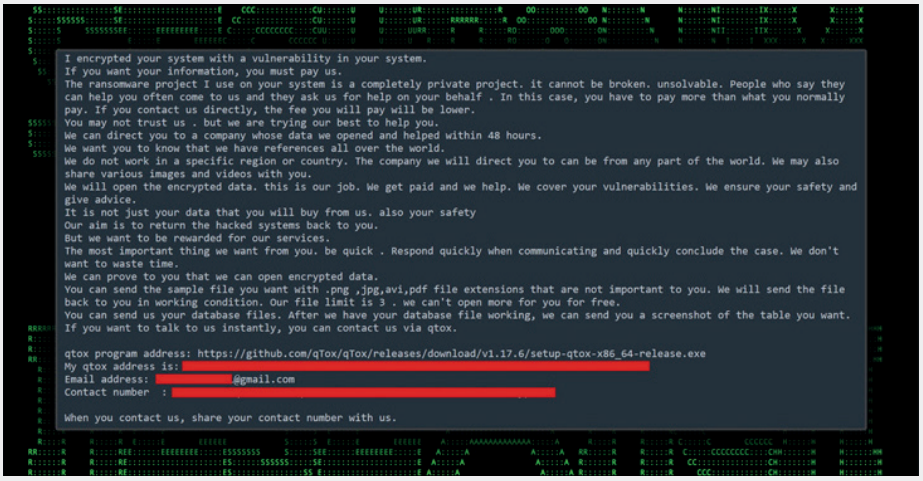
Eine 2022-Umfrage von Hiscox ergab, dass sich US-Unternehmen mehr Sorgen über Cyberangriffe (46%) als über die Pandemie (43%) oder den Fachkräftemangel (38%) machen: Die Zahl der Cyberangriffe nimmt in den USA zu, wobei fast die Hälfte aller US-Unternehmen in den letzten 12 Monaten Opfer eines Cyberangriffs geworden ist.

„Sicherheits- und Cybersicherheitsvorfälle sind kostspielig, und die Verluste steigen von Jahr zu Jahr. Der FBI-Bericht zur Internetkriminalität zeigt zum Beispiel, dass die Verluste durch Internetkriminalität im Jahr 2022 mehr als $10 Mrd. USD betragen werden, gegenüber $3,5 Mrd. USD im Jahr 2019. Auch wenn diese Verluste erschütternd sind, sind sie mit Sicherheit nur die Spitze des Eisbergs. Sie spiegeln nur Verluste wider, die dem FBI gemeldet werden, und viele Opfer – ob Privatpersonen oder Unternehmen – entscheiden sich, keine Anzeige zu erstatten oder Verluste zu melden. Außerdem sind in den FBI-Daten bestimmte Arten von Verlusten, wie z.B. Ransomware-Zahlungen, nicht enthalten. Zusätzlich zu den direkten Kosten entstehen den Opfern oft indirekte Kosten, wie z.B. Umsatzeinbußen aufgrund von Ausfallzeiten, Ruf- oder Markenschäden sowie der Verlust von Geschäftsgeheimnissen oder geistigem Eigentum. Diese können die Höhe der direkten Kosten leicht übersteigen. Angesichts dieser wachsenden Bedrohungen ist es nicht verwunderlich, dass Unternehmen in allen Branchen die Sicherheit immer wieder als oberste Priorität für neue Ausgaben angeben." (Quelle: Avasant, 2023)

Basierend auf einer Ende 2022 von der Enterprise Strategy Group durchgeführten Studie planen 65% der Unternehmen, ihre Ausgaben für Cybersicherheit im Jahr 2023 zu erhöhen, wobei 40% der Befragten angaben, dass die Verbesserung der Cybersicherheit die wichtigste Rechtfertigung für IT-Investitionen ist.

„Unabhängig von der Branche sind kleine und mittlere Unternehmen (KMU) ein Hauptziel für Cyberangriffe. Es besteht der Irrglaube, dass große Unternehmen ein großes Ziel sind, aber die Realität ist, dass kleinere Organisationen oft nicht über die richtigen Sicherheitsprotokolle verfügen, sodass sie anfälliger für Angriffe sind.... Derzeit geben kleine und mittlere Unternehmen nur 10% ihres jährlichen IT-Budgets für Dienstleistungen und Lösungen von Cybersicherheitsunternehmen aus... Diese Budgetierung entspricht nicht der raschen Zunahme von Cyberangriffen... Es ist klar, dass die Ausgaben für Cybersicherheit im Jahr 2023 und in den darauf folgenden Jahren steigen werden. In unseren Cybersecurity-Prognosen für 2023 haben wir festgestellt, dass die Zahl der Cyberangriffe von 2021 bis 2022 um 15% gestiegen ist. 2023 wird dieser Anstieg voraussichtlich noch höher ausfallen. Raffiniertere Cyberangriffe durch künstliche Intelligenz oder Geo-Phishing werden die Unternehmen zu höheren Ausgaben zwingen." (Quelle: BIO-key, 2023)

"Cyberkriminalität ist eine ernstzunehmende Bedrohung, um die man sich kümmern muss... In den letzten Jahren haben sich die Prioritäten der Unternehmen weltweit deutlich verschoben, wobei Cyberangriffe eine der größten Sorgen darstellen. Experten schätzen, dass die Gesamtkosten der Cyberkriminalität in diesem Jahr $8 Billionen USD erreichen werden. Zweifelsohne steht die Cybersicherheit ganz oben auf der Agenda der Branchenführer. Außerdem werden die Cyberkriminellen immer raffinierter, sodass es schwierig ist, diese Bedrohungen abzuwehren. Dies ist einer der Hauptgründe, warum immer mehr Unternehmen Opfer von Cyberkriminellen werden. Daher ist es für Unternehmen wichtig, ihre Investitionen in Cybersicherheitsmaßnahmen zu erhöhen... Die USA sind die größte geografische Region für Cybersicherheitsausgaben im Jahr 2023... Dicht gefolgt von Westeuropa, das derzeit die zweitgrößte Region bei den Cybersicherheitsausgaben ist... Auch im asiatisch-pazifischen Raum wurden in diesem Jahr erhebliche Investitionen in die Cybersicherheit getätigt... Ab 2022 werden Unternehmen weltweit 9,9% ihrer IT-Budgets für Cybersicherheit ausgeben... Darüber hinaus wendet ein kleines Unternehmen im Durchschnitt etwa 5% seines IT-Budgets für Cybersicherheit auf. Dies zeigt, dass kleine und mittlere Unternehmen die Bedeutung der Cybersicherheit noch immer nicht verstanden haben... Rund 47% der kleinen Unternehmen haben kein Budget für Cybersicherheit... Dies zeigt, dass sie anfälliger für Cyberangriffe und Sicherheitsverletzungen sind... Es wird geschätzt, dass kleine und mittlere Unternehmen (KMU) im Jahr 2025 etwa $29,8 Mrd. USD für verwaltete Sicherheitsdienste ausgeben werden. Es wurde jedoch prognostiziert, dass sie $90 Mrd. USD für Cybersicherheit ausgeben werden. Das sind $33 Mrd. USD mehr als die $57 Mrd. USD im Jahr 2020... Ein erheblicher Teil der Unternehmen weltweit (73%, um genau zu sein) plant, seine Ausgaben für Cybersicherheit im Jahr 2023 zu erhöhen... Von den großen Unternehmen wagen es nur 7%, Risiken einzugehen und weniger als $250.000 USD pro Jahr in Cybersicherheit zu investieren... Währenddessen befinden sich 43% der großen Unternehmen in einem mittleren Bereich und investieren jährlich zwischen $250.000 und $999.999 USD in die Cybersicherheit... Google hat angekündigt, innerhalb von 5 Jahren über $10 Mrd. USD in die Verbesserung der Cybersicherheit zu investieren..." (Quelle, 2023)



Wenn Sie auf Ihrem Computerbildschirm eine Meldung wie die hierüber Abgebildete sehen, bedeutet dies, dass Ihr System durch einen Cyberangriff kompromittiert wurde und Sie oder Ihr Unternehmen in eine prekäre Lage geraten sind. Bedauerlicherweise sehen sich zahlreiche Personen und Unternehmen mit begrenzten Alternativen konfrontiert und sehen sich möglicherweise gezwungen, sich auf Cyberkriminelle einzulassen und deren Lösegeldforderungen zu erfüllen. (Bild aud em Artikel "Threat Actors Targeting Microsoft SQL Servers to Deploy FreeWorld Ransomware", 2023)

Die weltweiten Ausgaben für Cybersicherheit werden in diesem Jahr $219 Mrd. USD erreichen und in den nächsten 3 Jahren auf fast $300 Mrd. USD anwachsen, so die jüngste Prognose von IDC Data and Analytics. Es wird erwartet, dass die diesjährigen Investitionen in Hardware, Software und Dienstleistungen im Bereich der Cybersicherheit im Vergleich zu 2022 um 12,1% steigen und das Wachstum der gesamten IT-Ausgaben übertreffen werden. „Nahezu alle Branchen und Unternehmensgrößen werden bis 2026 ein niedriges zweistelliges Ausgabenwachstum verzeichnen, angetrieben durch die Ausweitung von Cloud- und Container-Implementierungen, die Notwendigkeit, den Fernzugriff auf Ressourcen zu sichern, und die Compliance-Anforderungen von Gesetzen zum Schutz der Privatsphäre und des Datenschutzes", sagt Serena Da Rold, Associate Research Director bei IDC. Die Analysten gehen davon aus, dass der Markt für Cybersicherheit sein anhaltendes Wachstum fortsetzen wird und dass die größten Ausgaben für Cybersicherheit in diesem Jahr auf Unternehmen aus den Bereichen Banken, Fertigung, professionelle Dienstleistungen und Regierungen entfallen werden, die mehr als ein Drittel aller Ausgaben für Cybersicherheit tätigen. Laut IDC wird Software, das am schnellsten wachsende Segment, in diesem Jahr 47% aller Ausgaben ausmachen, gefolgt von Dienstleistungen (39%) und Hardware (13%).

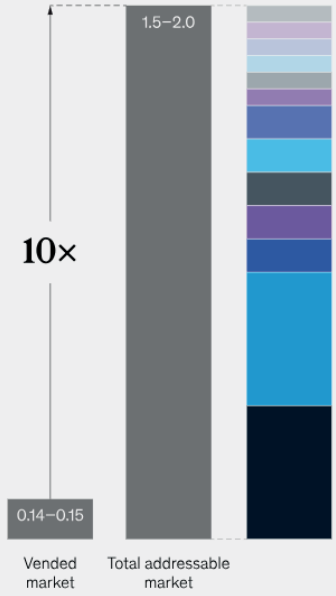
Unternehmen, die Cybersicherheitsprodukte verkaufen, stehen vor einer glänzenden Zukunft, die durch den ständig wachsenden Bedarf an robusten Cybersicherheitsmaßnahmen bestimmt wird. Da Cyberbedrohungen immer raffinierter und allgegenwärtiger werden, werden sich Unternehmen und Einzelpersonen zunehmend an Cybersecurity-Lösungen wenden, um ihre digitalen Werte und ihre Privatsphäre zu schützen.

Auszüge aus "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers" (McKinsey, 2022):

„Cyberangriffe nehmen zu und verursachen jedes Jahr Schäden in Billionenhöhe. Die Cybersicherheitsbranche hat die Chance, die Gelegenheit zu ergreifen und zu nutzen. In dem Maße, wie die digitale Wirtschaft wächst, wächst auch die digitale Kriminalität. Die steigende Zahl von Online- und mobilen Interaktionen schafft Millionen von Angriffsmöglichkeiten. Viele davon führen zu Datenverletzungen, die sowohl Menschen als auch Unternehmen bedrohen. Bei der derzeitigen Wachstumsrate wird sich der Schaden durch Cyberangriffe bis 2025 auf etwa $10,5 Billionen USD jährlich belaufen – ein Anstieg um 300% gegenüber 2015. Angesichts dieses Cyberansturms werden Unternehmen weltweit im Jahr 2021 rund $150 Mrd. USD für Cybersicherheit ausgeben, was einem jährlichen Wachstum von 12,4% entspricht. Angesichts des Ausmaßes des Problems ist jedoch selbst dieses „Sicherheits-Wachrütteln" wahrscheinlich nicht ausreichend. Eine Umfrage unter 4.000 mittelständischen Unternehmen deutet darauf hin, dass sich das Bedrohungsvolumen von 2021 bis 2022 fast verdoppeln wird. Der Umfrage zufolge wurden fast 80% der beobachteten Bedrohungsgruppen, die im Jahr 2021 operieren, und mehr als 40% der beobachteten Malware noch nie zuvor gesehen. Diese Dynamik deutet auf ein erhebliches Potenzial in einem sich entwickelnden Markt hin. Die derzeit verfügbaren kommerziellen Lösungen erfüllen die Kundenanforderungen nicht vollständig... Infolgedessen klafft heute eine große Lücke zwischen dem $150-Mrd.-USD-Verkaufsmarkt und einem vollständig adressierbaren Markt. Bei einer heutigen Marktdurchdringung von etwa 10% der Sicherheitslösungen

The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.

Global cybersecurity market size, 2021, $ trillion

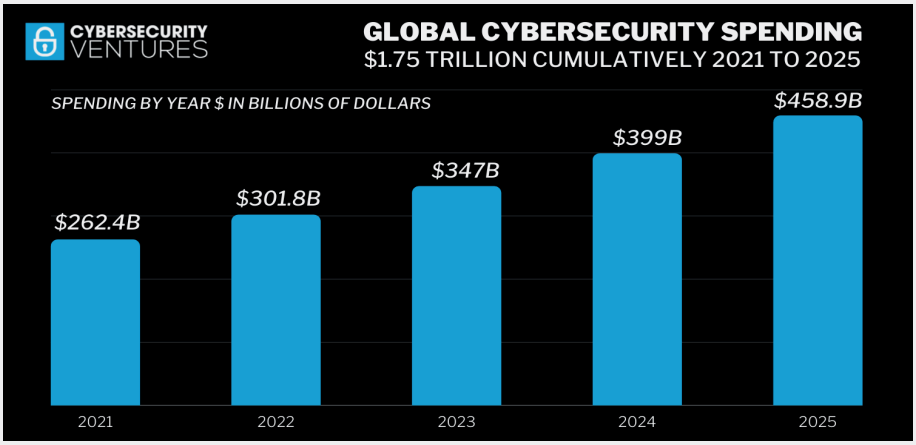


Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

Riesige Lücke zu schließen: Der adressierbare Markt stellt den kommerziellen Aspekt der Cybersicherheitsbranche dar, auf dem Organisationen und Einzelpersonen eine breite Palette von Cybersicherheitslösungen und -dienstleistungen zum Schutz vor Cyberbedrohungen erwerben können.

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

Die Wachstumsaussichten für Anbieter auf dem Cybersicherheitsmarkt sind außerordentlich vielversprechend, angetrieben durch die sich ständig erweiternde Bedrohungslandschaft, die zunehmende Digitalisierung in allen Branchen, strenge regulatorische Anforderungen und das wachsende Bewusstsein für die entscheidende Rolle der Cybersicherheit beim Schutz von Daten, Privatsphäre und digitalen Werten.



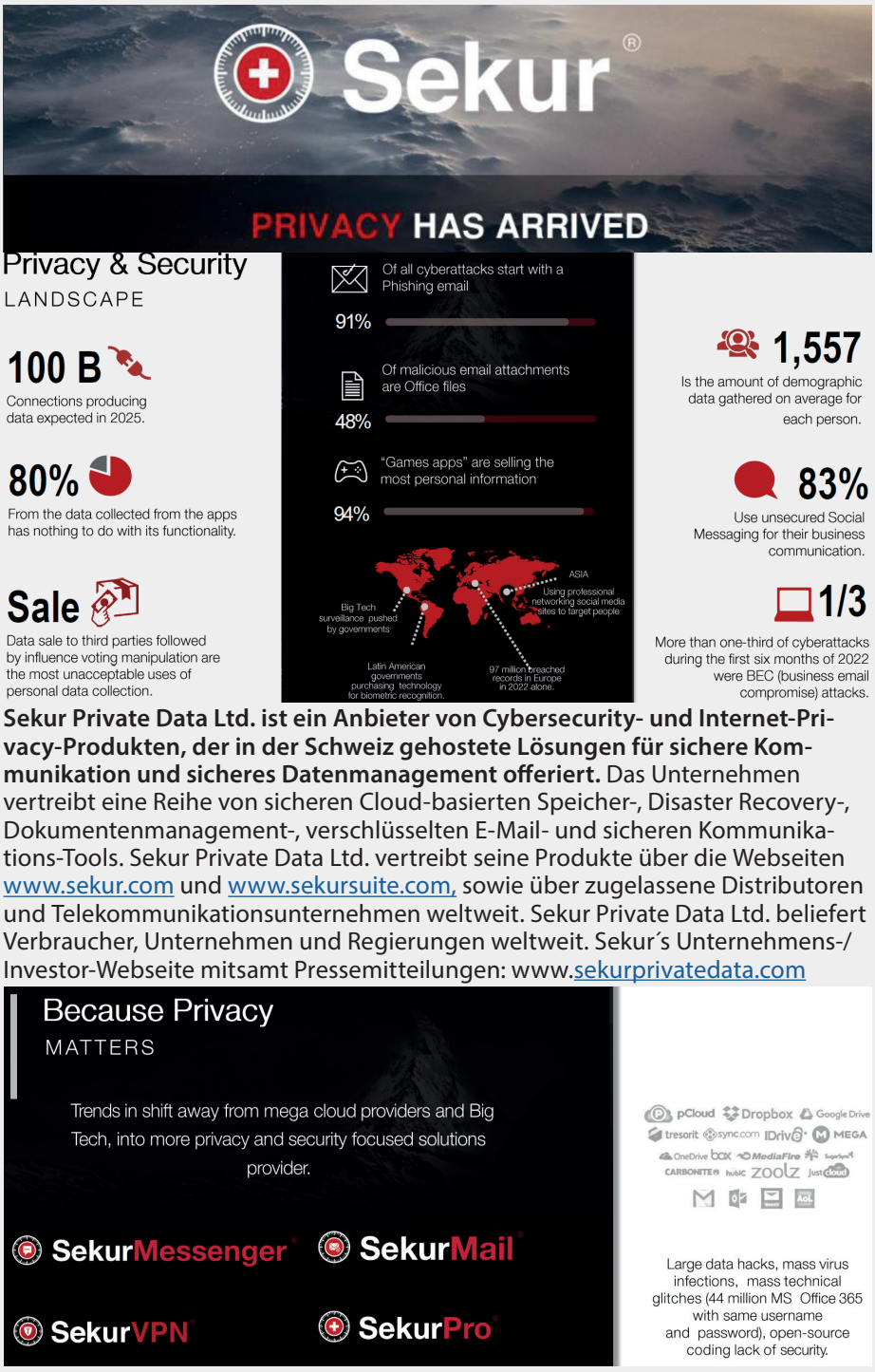
"Die Notwendigkeit, zunehmend digitalisierte Unternehmen, Internet-of-Things-Geräte (IoT) und Verbraucher vor Cyberkriminalität zu schützen, wird die weltweiten Ausgaben für Cybersicherheitsprodukte und -dienstleistungen im Fünfjahreszeitraum von 2021 bis 2025 auf insgesamt $1,75 Billionen USD ansteigen lassen, so Cybersecurity Ventures... Da prognostiziert wird, dass Cyberkriminalität die Welt bis 2025 jährlich $10,5 Billionen USD kosten wird, gegenüber $3 Billionen USD vor einem Jahrzehnt und $6 Billionen USD im Jahr 2021, wird ein entsprechendes Wachstum der Ausgaben für Cybersicherheit entscheidend sein, um Schritt zu halten... Die Cybersicherheit ist der einzige Posten, für den es theoretisch kein Ausgabenlimit gibt... Es gibt ein Budget, bevor ein Unternehmen von einem Cyberangriff oder einer Reihe von Angriffen betroffen ist, und dann gibt es die tatsächlichen Ausgaben, die danach getätigt werden. Welches Unternehmen oder welcher Verbraucher würde nicht alles tun und ausgeben, was nötig ist, um sich von einem Hackerangriff zu erholen? Die Märkte werden jedoch nicht durch unbegrenzte Budgets oder die außergewöhnlichen Maßnahmen bestimmt, zu denen Unternehmen bereit sind, wenn es hart auf hart kommt, aber das ist eine der Dynamiken im aufkeimenden Cybersicherheitsbereich... Während alle anderen Technologiesektoren durch die Reduzierung von Ineffizienzen und die Steigerung der Produktivität angetrieben werden, werden die Ausgaben für Cybersicherheit durch Cyberkriminalität angetrieben..." (Quelle)

beläuft sich die Gesamtchance auf einen erstaunlichen adressierbaren Markt von $1,5 bis $2 Billionen USD... Dies bedeutet nicht, dass der Markt diese Größe in absehbarer Zeit erreichen wird (die aktuelle Wachstumsrate beträgt 12,4% pro Jahr, ausgehend von einer Basis von ca. $150 Mrd. USD im Jahr 2021), sondern vielmehr, dass ein solch massives Delta die Anbieter und Investoren dazu zwingt, mehr Wirkung bei den Kunden zu erzielen, indem sie die Bedürfnisse unterversorgter Segmente besser erfüllen, die Technologie kontinuierlich verbessern und die Komplexität reduzieren – und das derzeitige Käuferklima könnte einen einzigartigen Moment für Innovationen in der Cybersicherheitsbranche darstellen."

Internetnutzer genießen oft die Vorteile von Komfort, Zuverlässigkeit und Skalierbarkeit, wenn sie Dienste von Mega-Cloud-Anbietern und großen Technologieunternehmen nutzen. Es gibt jedoch mehrere Probleme und Nachteile, die mit der starken Abhängigkeit von diesen Unternehmen verbunden sind. Die Nutzer sollten sich der potenziellen Nachteile bewusst sein, die mit der Dominanz dieser Unternehmen in der Technologiebranche verbunden sind:

Datenschutz-Bedenken
Mega-Cloud-Anbieter und große Technologieunternehmen sammeln in der Regel große Mengen an Nutzerdaten für verschiedene Zwecke, einschließlich gezielter Werbung. Dies wirft erhebliche Datenschutzbedenken auf, da sich die Nutzer mit dem Ausmaß der Überwachung und Datenverfolgung durch diese Unternehmen unwohl fühlen können.

Risiken für die Datensicherheit
Obwohl diese großen Technologieunternehmen stark in Sicherheitsmaßnahmen investieren, sind sie dennoch attraktive Ziele für Cyberangriffe. Eine Sicherheitsverletzung kann zur Preisgabe sensibler Benutzerdaten führen, was wiederum Identitätsdiebstahl, Betrug und andere sicherheitsrelevante Probleme zur Folge haben kann. In den letzten Jahren kam es zu großen Datenhacks, massenhaften Vireninfektionen und massenhaften technischen Pannen, die nicht nur auf mangelnde Sicherheit bei Open-Source-Codes zurückzuführen sind.

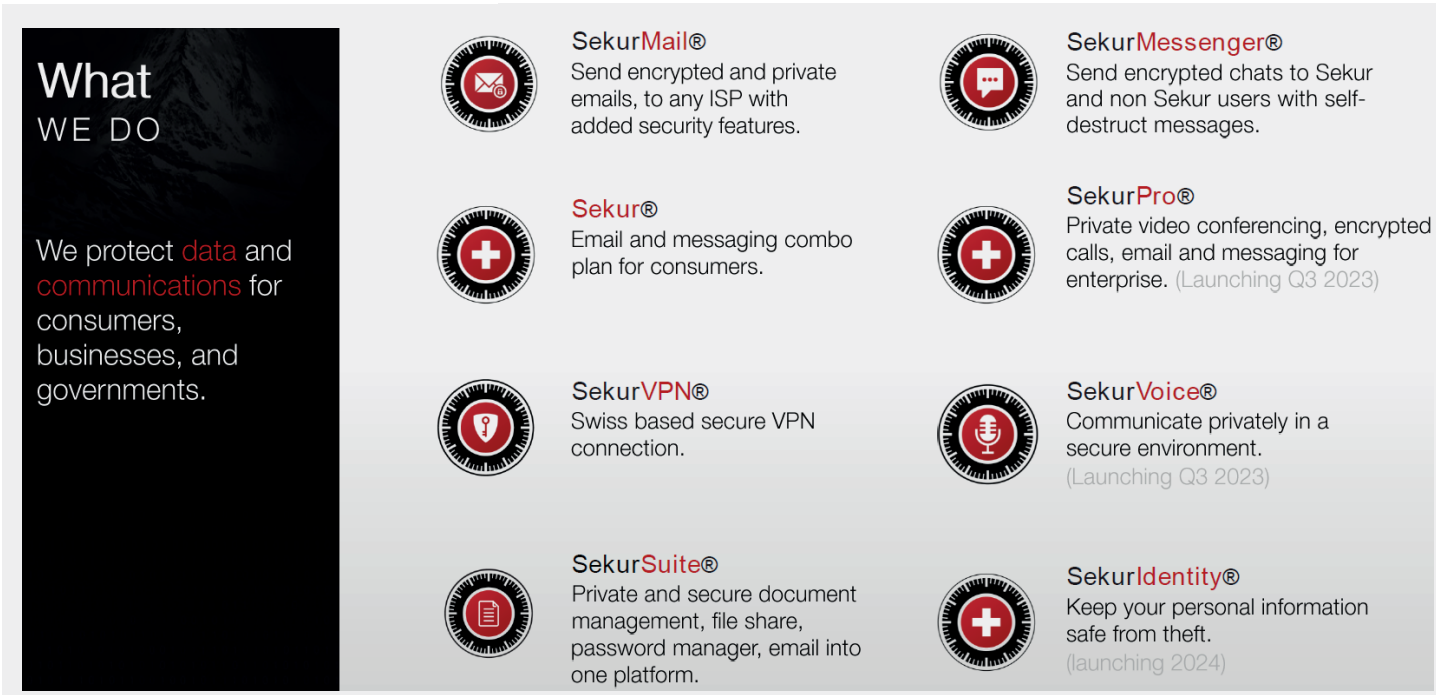


Sekur Private Data Ltd. ist ein Anbieter von Cybersecurity- und Internet-Privacy-Produkten, der in der Schweiz gehostete Lösungen für sichere Kommunikation und sicheres Datenmanagement offeriert. Das Unternehmen vertreibt eine Reihe von sicheren Cloud-basierten Speicher-, Disaster Recovery-, Dokumentenmanagement-, verschlüsselten E-Mail- und sicheren Kommunikations-Tools. Sekur Private Data Ltd. vertreibt seine Produkte über die Webseiten www.sekur.com und www.sekursuite.com, sowie über zugelassene Distributoren und Telekommunikationsunternehmen weltweit. Sekur Private Data Ltd. beliefert Verbraucher, Unternehmen und Regierungen weltweit. Sekur´s Unternehmens-/Investor-Webseite mitsamt Pressemitteilungen: www.sekurprivatedata.com

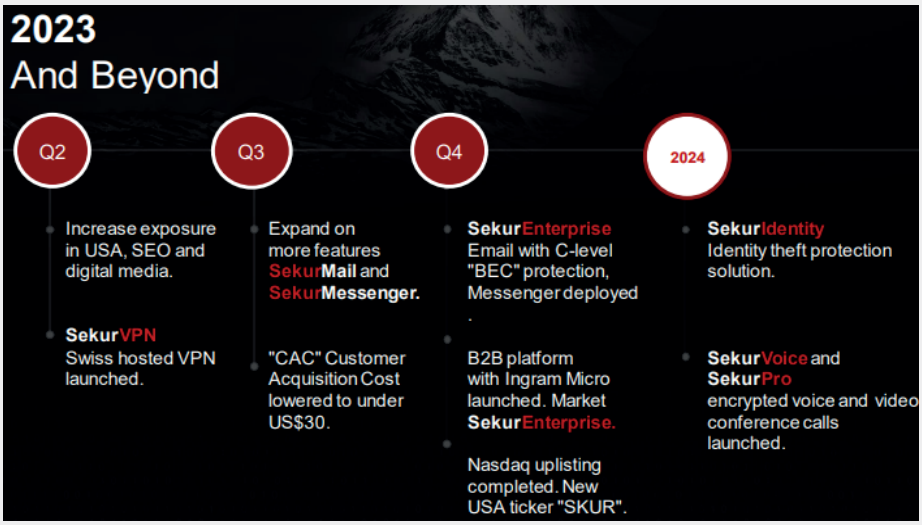
Ausfälle von Diensten
Selbst die größten Cloud-Anbieter und Technologieunternehmen sind nicht vor Serviceausfällen gefeit. Nutzer, die sich in hohem Maße auf diese Dienste verlassen, können in ihren täglichen Abläufen gestört werden, wenn bei diesen Unternehmen technische Probleme oder Ausfallzeiten auftreten.

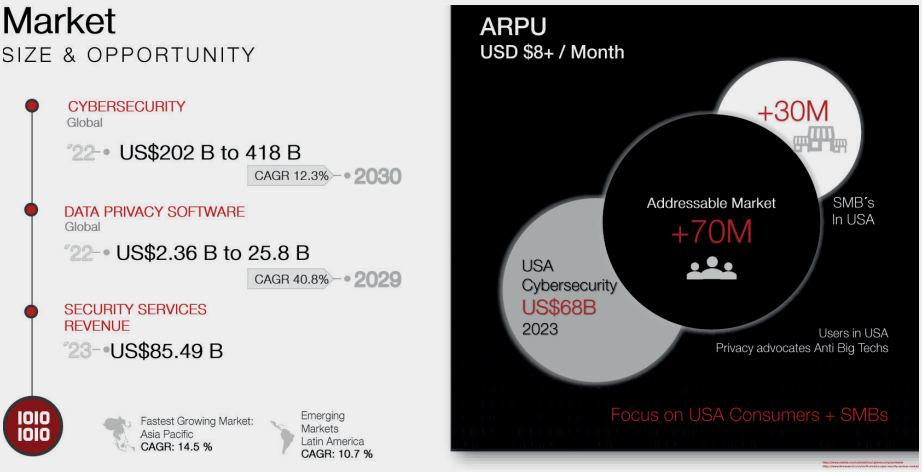
Begrenzter Kundensupport
Aufgrund ihrer Größe haben Mega-Cloud-Anbieter und große Technologieunternehmen unter Umständen Schwierigkeiten, allen ihren Nutzern einen persönlichen Kundensupport zu bieten. Dies kann zu Frustration bei den Nutzern führen, die Probleme haben oder Unterstützung benötigen.

Regulatorische Kontrolle
Mega-Cloud-Anbieter und große Technologieunternehmen sind häufig mit behördlichen Kontrollen und kartellrechtlichen Untersuchungen konfrontiert. Dies kann zu rechtlichen Streitigkeiten, Geldstrafen und Änderungen der Geschäftspraktiken führen, die sich auf das Nutzererlebnis auswirken können.



Sekur Private Data Ltd. wurde gegründet, um die Nachteile von großen Technologieunternehmen und Mega-Cloud-Anbietern zu vermeiden. Sekur schützt Daten und Kommunikation für Privatpersonen, Unternehmen und Regierungen. Sekur bietet Privatsphäre und Sicherheit kombiniert an – mit Kommunikationslösungen, die Ende-zu-Ende verschlüsselt sind und ohne soziales Engagement, Location Mining und Big-Tech-Data-Mining-Eingriffe. Dies schützt die Privatsphäre der Benutzer ohne Metadaten oder Cache in ihren Geräten. Alle Unterhaltungen sind in Sekur´s Virtual-Vault® und Helix® Technologie eingeschlossen.





Im Gegensatz zu vielen anderen Anbietern, besitzt Sekur 100% der Infrastruktur (keine Amazon Web Services, Google Cloud oder Microsoft Azure). Der gesamte Datenverkehr wird in der Schweiz gehostet, unter Verwendung einer proprietären Closed-Source-Technologie, einer unabhängigen Plattform, die nicht von Big Tech abhängig ist, einer militärischen Verschlüsselung und unter Berücksichtigung der Schweizer Datenschutzgesetze. Alle Benutzerdaten sind durch das Schweizerische Bundesgesetz über den Datenschutz (DSG) und die Eidgenössische Datenschutzverordnung geschützt, die einen der stärksten Schutz der Privatsphäre in der Welt sowohl für Einzelpersonen als auch für Unternehmen bietet. Die hochmodernen Computer- und Speicherserver von Sekur befinden sich in ISO-zertifizierten, von Schweizer Banken zugelassenen Datenzentren mit allen Sicherheitsvorkehrungen, die Sie von Datenzentren in der Schweiz erwarten würden, die einige der größten Banken und Organisationen der Welt bedienen. Das Netzwerk von Sekur ist durch eine Firewall der Enterprise-Klasse geschützt und beinhaltet eine SSL-Verschlüsselung, um Ihre Daten zu schützen.

WARUM SCHWEIZ

Die Schweiz verfügt über die weltweit strengsten Datenschutzgesetze, das DSG. Der Zweck des DSG ist der Schutz der Privatsphäre, der Interessen und der Grundrechte der betroffenen Personen. Ende September 2020, nach einem fast vierjährigen Gesetzgebungsverfahren, haben beide Kammern des Schweizer Parlaments das revidierte Bundesgesetz über den Datenschutz (revidiertes DSG) verabschiedet. Das revidierte DSG enthält zahlreiche Anpassungen an die EU-Datenschutzgrundverordnung (DSGVO), behält aber seine eigene Grundkonzeption bei und weicht in verschiedenen Aspekten von der DSGVO ab. Beispiele für wichtige Änderungen im revidierten DSG sind: Deutlich verschärfte Sanktionen, erweiterte Informationspflichten, die Pflicht zur Erstellung eines Verzeichnisses der Datenbearbeitungsaktivitäten und die Erweiterung der Rechte der betroffenen Person.

Die Schweiz verfügt über eine stabile, florierende und hochtechnologische Wirtschaft und genießt großen Wohlstand. In mehreren Rankings wird sie als eines der wohlhabendsten Länder der Welt (pro Kopf) eingestuft. Der Global Competitiveness Report des Weltwirtschaftsforums stuft die Schweizer Wirtschaft derzeit als eine der wettbewerbsfähigsten der Welt ein. Die Schweiz ist auch Sitz mehrerer großer multinationaler Unternehmen und Nichtregierungsorganisationen, darunter die Weltgesundheitsorganisation und die Vereinten Nationen.

Strenge Datenschutzgesetze

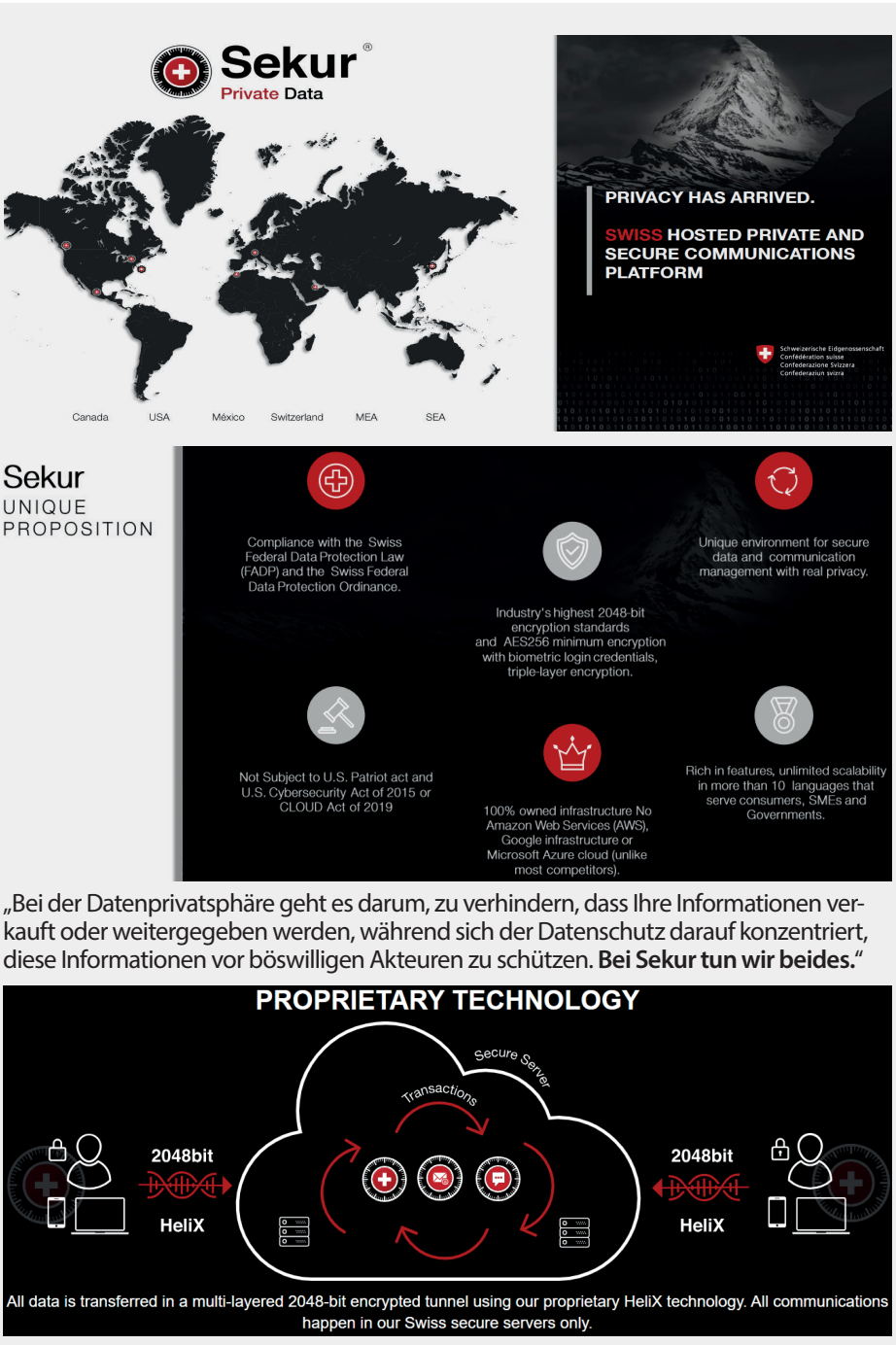
Die Schweiz hat die strengsten Datenschutzgesetze der Welt. Alle Nutzerdaten sind durch das Schweizerische Bundesgesetz über den Datenschutz (DSG) und die Eidgenössische Datenschutzverordnung (EDÖB) geschützt, die sowohl für Einzelpersonen als auch für Unternehmen einen der strengsten Datenschutzgesetze der Welt bieten.

Neutralität

Die Schweiz kann auf eine lange Geschichte der Neutralität zurückblicken – seit 1815 hat sie keinen Krieg mehr geführt und ist in allen internationalen politischen Angelegenheiten neutral geblieben.

Politisch unabhängig

Die Schweiz bleibt in allen staatlichen und politischen Belangen unabhängig und ist nicht Mitglied der EU und des Europäischen Wirtschaftsraum Außerdem gehört sie zu den 5 Ländern, die im Index der wirtschaftlichen Freiheit am besten abschneiden.



„Bei der Datenprivatsphäre geht es darum, zu verhindern, dass Ihre Informationen verkauft oder weitergegeben werden, während sich der Datenschutz darauf konzentriert, diese Informationen vor böswilligen Akteuren zu schützen. **Bei Sekur tun wir beides.**“

Langanhaltende Stabilität

Die Schweiz hat eine Arbeitslosenquote von unter 5% und verfügt über das höchste Vermögen pro Erwachsenem in der Welt. Sie wird als eine der 5 effizientesten Volkswirtschaften der Welt eingestuft.

Geringe Netzwerk-Latenzzeit

Die Lage der Schweiz ist für jeden Betrieb von Vorteil, da die Entfernungen innerhalb Europas kurz sind und die Schweiz zwischen Asien/Mittlerer Osten und Nordamerika liegt.

Geringe Umweltrisiken

Die Schweiz ist nicht anfällig für Umweltrisiken wie Wirbelstürme, Tsunamis, Vulkane, Erdbeben, Waldbrände oder Überschwemmungen. 2016 schrieb die Schweiz Geschichte, als sie als erstes Land für die Einführung einer grünen Wirtschaft stimmte. Zu den neuen Initiativen gehörte das Ziel, bis 2050 die OneEarth-Nachhaltigkeit zu erreichen, indem „100% erneuerbare Energien, der Schutz und die Wiederherstellung von 50% der Böden und Ozeane der Welt sowie der Übergang zu einer regenerativen, kohlenstoffnegativen Landwirtschaft“ erreicht werden.

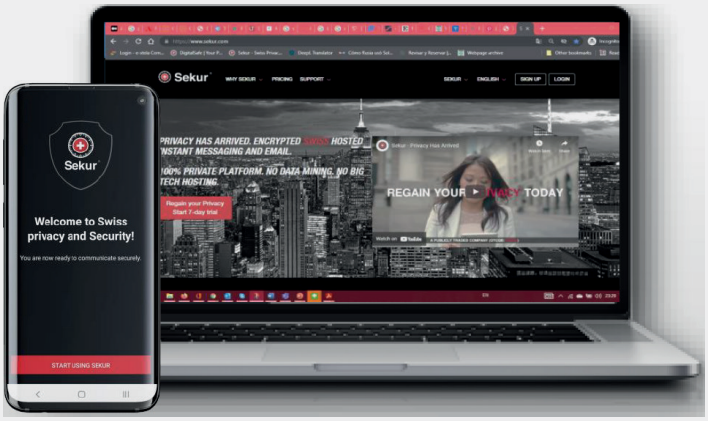
DIE CHANCE

"Die Cybersicherheit macht inzwischen einen beträchtlichen Teil des Budgets eines Unternehmens aus. Tatsächlich schätzt Gartner, dass Unternehmen in den nächsten 5 Jahren $1,75 Billionen USD für Cybersicherheit ausgeben werden. Dies ist ein beträchtlicher Anstieg für eine Branche, die im Jahr 2004 nur $3,5 Milliarden USD wert war... Von 2020 bis 2021 steigen die Ausgaben für Cybersicherheit exponentiell an... Im Jahr 2021 ist ein erheblicher Anstieg der Ausgaben für die Sicherung von Geräten außerhalb des Firmengeländes zu verzeichnen. Es wird prognostiziert, dass bis Ende 2024 die Ausgaben für mobile Sicherheit $7,2 Mrd. USD übersteigen werden... Smartphones sind zu einem integralen Bestandteil des Lebens geworden, daher ist die Einbeziehung der mobilen Sicherheit in die Cybersicherheitsrichtlinien der meisten Unternehmen mittlerweile unerlässlich. Es wird sogar prognostiziert, dass fehlende mobile Sicherheit eine der am schnellsten wachsenden Bedrohungen im Bereich der Cybersicherheit sein wird, da sie potenzielle Schwachstellen birgt... Da sich die technologische Landschaft ständig weiterentwickelt und die staatlichen Vorschriften immer strenger werden, erhöhen die Unternehmen ihr Budget für Cybersicherheit stetig." (Quelle, 2022)

EINES DER PROBLEME

„79% der Internetnutzer in Amerika sind besorgt über den Datenschutz, 41% der US-Nutzer löschen häufig Cookies und 30% der Verbraucher haben Adblocker heruntergeladen." (Quelle)

Letzten Monat im August kündigten die US-Regulierungsbehörden Strafen in Höhe von insgesamt $549 Mio. USD gegen 15 Finanzunternehmen an, weil sie „weit verbreitete und langjährige Versäumnisse" bei der elektronischen Aufzeichnung der Mitarbeiterkommunikation begangen hatten, darunter auch die Nutzung unbeaufsichtigter Kanäle wie der Messaging-Apps WhatsApp und Signal zur Besprechung von Unternehmensangelegenheiten. Die SEC (Securities and Exchange Commission) und die CFTC (Commodity Futures Trading Commission) haben Anklagen und Geldstrafen gegen Wells Fargo, Société Générale, BNP Paribas, Bank of Montreal, BMO Capital Markets und andere Unternehmen wegen der Verwendung nicht genehmigter Kommunikationsmethoden bekanntgegeben. **Letztes Jahr im September verhängte die SEC gegen 16 Finanzunternehmen Geldstrafen in Höhe von insgesamt $1,1 Mrd. USD,** weil sie es versäumt hatten, ihre elektronische Kommunikation aufzubewahren, darunter Barclays, Bank of America, Citigroup, Credit Suisse, Goldman Sachs, Morgan Stanley und UBS.



"79% der Internetnutzer in Amerika sind besorgt über den Datenschutz, 41% der US-Nutzer löschen häufig Cookies und 30% der Verbraucher haben Adblocker heruntergeladen." (Quelle)

Sekur hält Ihren Internetverkehr privat und sicher: Privatsphäre ist die neue Sicherheit!

Datenschutz: Schützt Ihre persönlichen Informationen und Kommunikationen vor dem Zugriff durch Unbefugte, wie Hacker, Werber oder unseriöse Agenturen.
Sicherheit: Verschlüsselung und andere Sicherheitsmaßnahmen, die verhindern, dass Ihre Nachrichten während der Übertragung oder im Ruhezustand abgefangen, verändert oder manipuliert werden.
Online-Freiheit: Ermöglicht es Ihnen, auf Informationen zuzugreifen und mit jedem auf der Welt zu kommunizieren, unabhängig von geografischen oder politischen Barrieren.

DIE LÖSUNG

Sekur hat ein überzeugendes Produktportfolio für Internetnutzer (Privatpersonen, Unternehmen und Regierungen) zum Schutz ihrer Daten auf den Markt gebracht, um die Sicherheit zu maximieren und die Anforderungen der Regulierungsbehörden zu erfüllen.

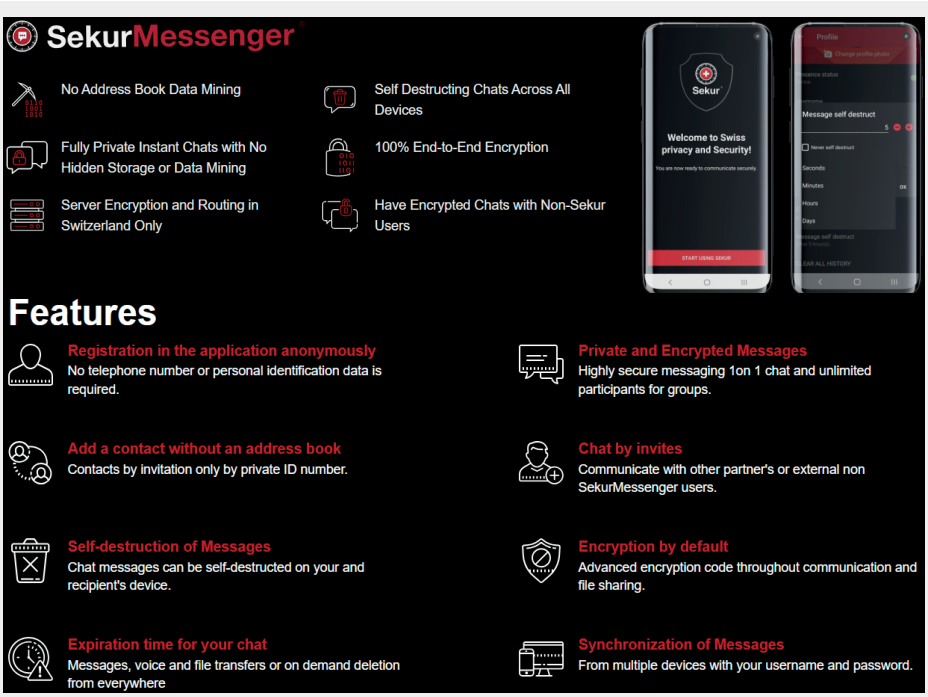
Letztes Jahr wurde der SekurMessenger zusammen mit dem América Móvil-Mobilfunkbetreiber Telcel in Mexiko auf den Markt gebracht, mit dem Ziel, unsichere und nicht private Messaging-Anwendungen nicht nur für Unternehmen, sondern auch für den Massenmarkt zu ersetzen: „Die jüngsten Datenschutzverletzungen in Messaging-Anwendungen und insbesondere in der WhatsApp-Anwendung haben eine gewisse Dringlichkeit für Unternehmen und Datenschützer geschaffen, ihre Kommunikation vor Cyberangriffen und Identitätsdiebstahl über mobile und Desktop-Geräte zu schützen... Telcel ist mit über 75 Mio. Mobilfunkteilnehmern der größte Mobilfunkbetreiber in Mexiko. América Móvil ist der siebtgrößte Telekommunikationsbetreiber der Welt mit über 277 Mio. Mobilfunkkunden in mehr als 20 Ländern Lateinamerikas und Europas. Die Aktien des Unternehmens werden an der New Yorker Börse unter dem Kürzel AMX gehandelt... Sobald die Verkäufe in Mexiko in Schwung kommen, soll die Einführung auf andere Länder ausgeweitet werden, in denen America Movil mit seiner Marke Claro tätig ist, wie Kolumbien, Peru und andere lateinamerikanische Länder, wenn das Geschäft in den nächsten Jahren wächst."

Bei Sekur werden alle Daten, einschließlich der Benutzerauthentifizierungsinformationen, über das Internet übertragen und auf den eigenen Servern in verschlüsselter Form gespeichert. Alle Verbindungen zu den Servern von Sekur sind für alle Benutzer mit 2048bit SSL-Verschlüsselung geschützt. Passwörter werden mit dem bcrypt-Algorithmus verschlüsselt. Das Sperren des Kontos

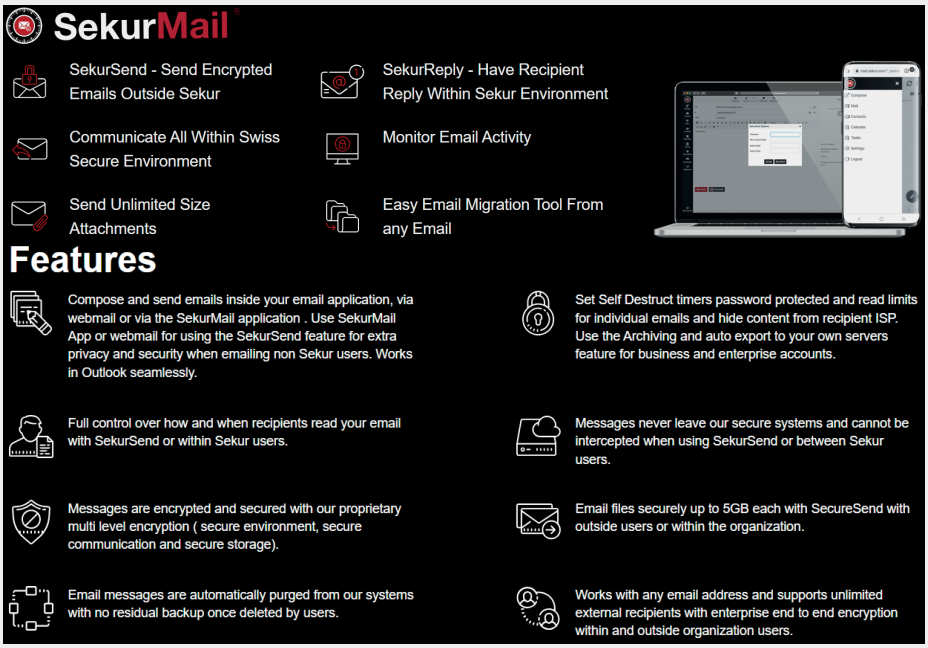
nach einer vordefinierten Anzahl von fehlgeschlagenen Anmeldeversuchen verhindert das Erraten von Passwörtern mit roher Gewalt. Zeitbasiertes Erraten von Passwörtern ist aufgrund der Natur der bcrypt-Verschlüsselung nicht möglich. Wenn die aktuelle Sitzung abläuft, wird das Browserfenster auf die Anmeldeseite umgeleitet, falls der Computer unbeaufsichtigt gelassen wird. Die Notizen werden auf dem Server mit einer AES-256-Verschlüsselung gespeichert und der Verschlüsselungsschlüssel wird auf einem separaten Server gespeichert, der nicht über das Internet zugänglich ist. Für die ultimative Sicherheit und den Schutz der Privatsphäre können die Benutzer ihr eigenes Passwort für die Verschlüsselung der Daten verwenden lassen. In diesem Fall ist es nicht möglich, die privaten Daten des Benutzers ohne Kenntnis des Passworts zu entschlüsseln. Nicht einmal Sekur-Mitarbeiter können die Daten entschlüsseln. Das bedeutet aber auch, dass das Passwort des Benutzers nicht zurückgesetzt werden kann und die Daten bei Verlust des Passworts für immer verloren sind.

Sekur speichert die Daten in einem erstklassigen Datazentrum in der Schweiz, das für seine strengen Standards und Qualitätskontrollen bekannt ist. Sekur verfügt über die notwendige physische Umgebung, um die Server 24 Stunden am Tag, 7 Tage die Woche in Betrieb zu halten, selbst bei Stromausfällen und größeren Naturkatastrophen. Diese erstklassigen Einrichtungen sind kundenspezifisch mit Doppelböden, HVAC-Temperaturkontrollsystemen mit separaten Kühlzonen und erdbebensicheren Racks ausgestattet. Sie bieten ein breites Spektrum an physischen Sicherheitsmerkmalen, darunter hochmoderne Rauchmelde- und Brandbekämpfungssysteme, Bewegungsmelder, einen rund um die Uhr gesicherten Zugang, Videokameraüberwachung und Alarme bei Sicherheitsverletzungen.

In Übereinstimmung mit dem **Payment Card Industry Data Security Standard** (PCI DSS) lässt Sekur seine Netzwerkinfrastruktur rund um die Uhr von Dritten überwachen, um bekannte Anwendungs- und Serviceschwachstellen aufzuspüren. Außerdem führt das Unternehmen jährlich ein mehrtägiges Vor-Ort-Audit durch, bei dem jeder Aspekt des Systems geprüft wird: Von der Software-Entwicklung bis zum Hardware-Einsatz, von der Personalpolitik bis zur Passwortverwaltung. Es gibt mehr als 200 Kriterien, die Sekur erfüllen muss, um sein Konformitätsniveau zu halten.



"Die jüngsten Datenschutzverletzungen bei Messaging-Anwendungen haben dazu geführt, dass Unternehmen und Datenschutz-Befürworter ihre Kommunikation über mobile und Desktop-Geräte dringend vor Cyberangriffen und Identitätsdiebstahl schützen müssen." (Quelle)



Sekur ist stolz darauf, die Daten der Benutzer in einem politisch und wirtschaftlich stabilen und neutralen Land zu speichern. Die Schweiz hält sich nicht an den USA PATRIOT ACT. Dies gewährleistet, dass Ihre Daten vor konkurrierenden Räubern oder Agenturen und Einrichtungen mit persönlichen Motiven, die Ihre Daten ausspähen würden, sicher sind.

SekurMessenger

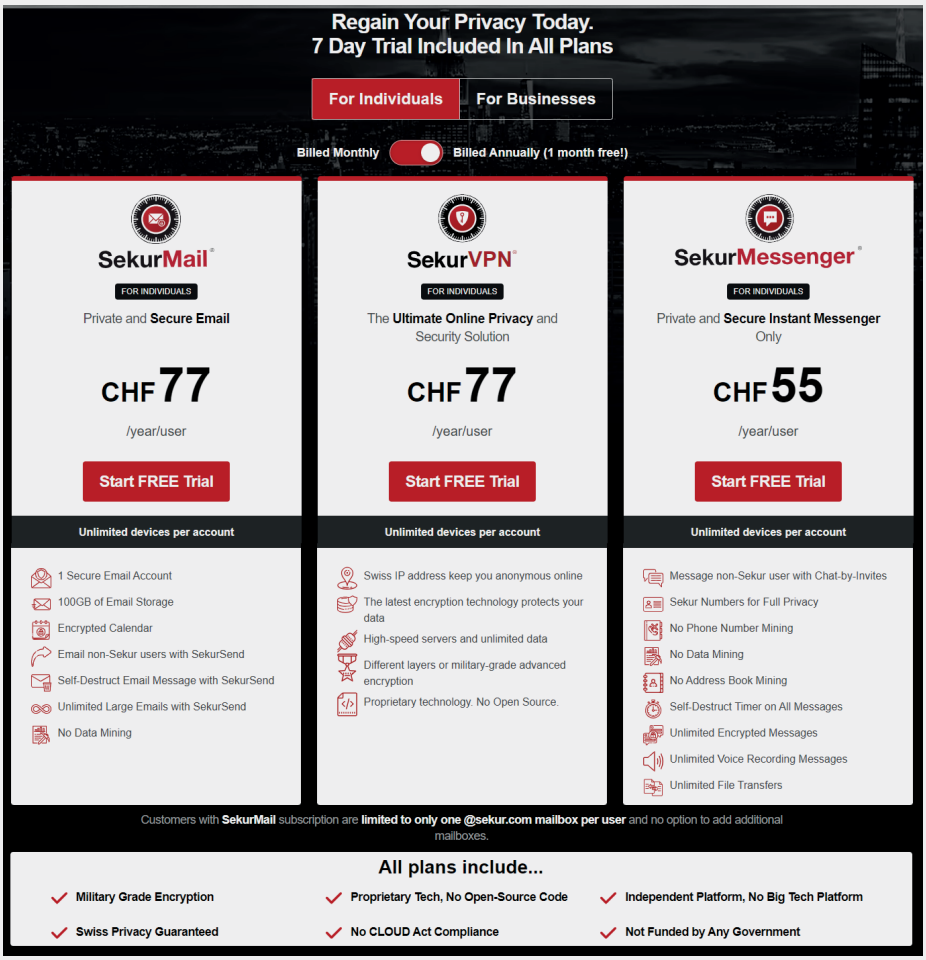
Verschlüsselte Messaging-Anwendung für Organisationen, die ihren Informationsfluss schützen und ihre Kommunikation zwischen Geräten, mit Kunden und Partnern sichern müssen. SekurMessenger ist keine gewöhnliche Messaging-App. Sie wurde entwickelt, um Verschlüsselung und Datenschutz auf militärischem Niveau zu bieten, indem sie sicherstellt, dass nur der Absender und der beabsichtigte Empfänger die ausgetauschten Nachrichten lesen können. Außerdem werden mehrere Verschlüsselungsebenen verwendet,

die die Daten der Benutzer in virtuellen Tresoren trennen und mit individuellen Schlüsseln verschlüsseln. Das bedeutet, dass Ihre Daten auch dann sicher sind, wenn eine Verschlüsselungsebene kompromittiert wird. Sekur sammelt und speichert keinerlei Metadaten, gibt keine Informationen an Dritte weiter und garantiert den Datenschutz durch eigene Server. SekurMessenger funktioniert sowohl für lizenzierte Nutzer der Anwendung als auch für externe Nutzer, die die App nicht besitzen. SekurMessenger bietet völlig private Instant-Chats ohne versteckte Speicherung oder Data-Mining. Das bedeutet, dass Ihre Unterhaltungen völlig privat gehalten werden und von niemandem sonst eingesehen werden können. SekurMessenger verwendet eine Ende-zu-Ende-Verschlüsselung, um sicherzustellen, dass Ihre Nachrichten sicher sind und von niemandem abgefangen werden können. Eines der Hauptmerkmale von SekurMessenger ist, dass es auf proprietärem Code ohne Open-Source aufgebaut ist. Das bedeutet, dass der Code, der für die Entwicklung von SekurMessenger verwendet wird, nicht öffentlich zugänglich ist und von niemandem verändert werden kann. Dies gewährleistet, dass der Dienst sicher ist und von niemandem kompromittiert werden kann.

SekurMail

Für jeden, der sich um Online-Datenschutz und Sicherheit kümmert, bietet SekurMail einen verschlüsselten Email-Service, der nicht nur standardmäßig privat ist, sondern auch ein sicheres und leistungsfähiges Werkzeug für die Kommunikation mit jedem, innerhalb oder außerhalb von Sekur. SekurMail verwandelt Ihre Email in eine sichere und private Kommunikationsplattform mit den höchsten Sicherheits- und Datenschutzstandards, indem es eine Ende-zu-Ende-Verschlüsselung für Nachrichten zwischen SekurMail-Benutzern und mit externen Benutzern verwendet. Die Backend-Email-Server von Sekur bieten die sicherste Umgebung für Ihre digitale Kommunikation. Zusätzlich zur mehrschichtigen Verschlüsselung verwendet Sekur proprietäre Technologien (Virtual Vault und Helix), um alle Daten, die auf Festplatten gespeichert sind, und alle Daten, die über das Netzwerk übertragen werden, zu verschlüsseln. Wenn ein Benutzer auf eine der Dienstleistungen von Sekur zugreift, verbindet er sich zuerst mit der sicheren Plattform des Unternehmens in seinem Rechenzentrum, und dann erfolgt die Transaktion innerhalb der Umgebung der eigenen Server. Dies eliminiert das Risiko, dass die

Laut einer auf Forbes veröffentlichten Umfrage nutzen 66% ein VPN, um persönliche Daten zu schützen, 80% nutzen ein VPN für mehr Sicherheit und 33% nutzen ein VPN, um ihre Internetaktivitäten zu verschleiern: „VPNs, oder virtuelle private Netzwerke, sind in der heutigen, vom Internet geprägten Welt unverzichtbare Werkzeuge geworden... VPNs werden verwendet, um Ihre IP-Adresse in öffentlichen Netzwerken zu sichern und zu verschlüsseln, und schützen Ihre Online-Aktivitäten vor Verfolgung und Ausbeutung durch Internet-Raubtiere. Ursprünglich wurden VPNs vor allem von einer Gruppe von Nischenunternehmen genutzt, doch in den letzten Jahren hat ihre Beliebtheit zugenommen. Die Akzeptanz bei Unternehmen und normalen Internetnutzern nimmt täglich zu. Der Schutz unserer Online-Privatsphäre und -Gewohnheiten ist heute wichtiger denn je...“



Seit der Markteinführung von SekurVPN im April 2023 und der Anpassung von „a-la-carte“-Paketen für Privat- und Geschäftskunden haben etwa 50% aller Kunden Pakete gekauft und 32% der Kunden haben SekurVPN im Paket oder einzeln gekauft. (Quelle)

Daten vom Gerät des Absenders abgefangen werden, d.h. die Daten können nicht gelesen oder abgerufen werden. Alle Daten in den Speichersystemen von Sekur sind verschlüsselt. Dies eliminiert „BEC" (Business Email Compromise) und Email-Phishing-Vorfälle.

SekurVPN

SekurVPN stellt eine sichere, verschlüsselte Verbindung zwischen Ihrem Gerät und dem Internet her und lässt Sie sicher und privat auf das Internet zugreifen, indem es Ihre Verbindung durch einen Server leitet und Ihre Online-Aktionen verbirgt. Alle Daten, die Sie senden und empfangen, bleiben vor neugierigen Blicken verborgen. Dazu gehören Ihr Internetdienstanbieter (ISP), potenzielle Hacker und sogar staatliche Überwachungsbehörden. Es kann Ihnen auch helfen, geografische Beschränkungen und Zensur zu umgehen. Der SekurVPN Software-Client auf dem Gerät des Benutzers verschlüsselt die Verbindungsanforderung des Geräts an den zugehörigen VPN-Server. Sobald die Verbindung hergestellt ist, werden die Informationsanfragen verschlüsselt und gehen vom Gerät des Benutzers zum VPN-Server. Der VPN-Server entschlüsselt die Anfrage und nutzt das Internet, um die Informationen zu erhalten. Nach der Beschaffung verschlüsselt der VPN-Server die Informationen und sendet sie zurück, die dann von der Client-Software entschlüsselt werden. Sekur verwendet seine eigenen VPN-Server in der Schweiz. Mit der unkomplizierten App können Sie überall auf der Welt blitzschnelle Verbindungsgeschwindigkeiten genießen.

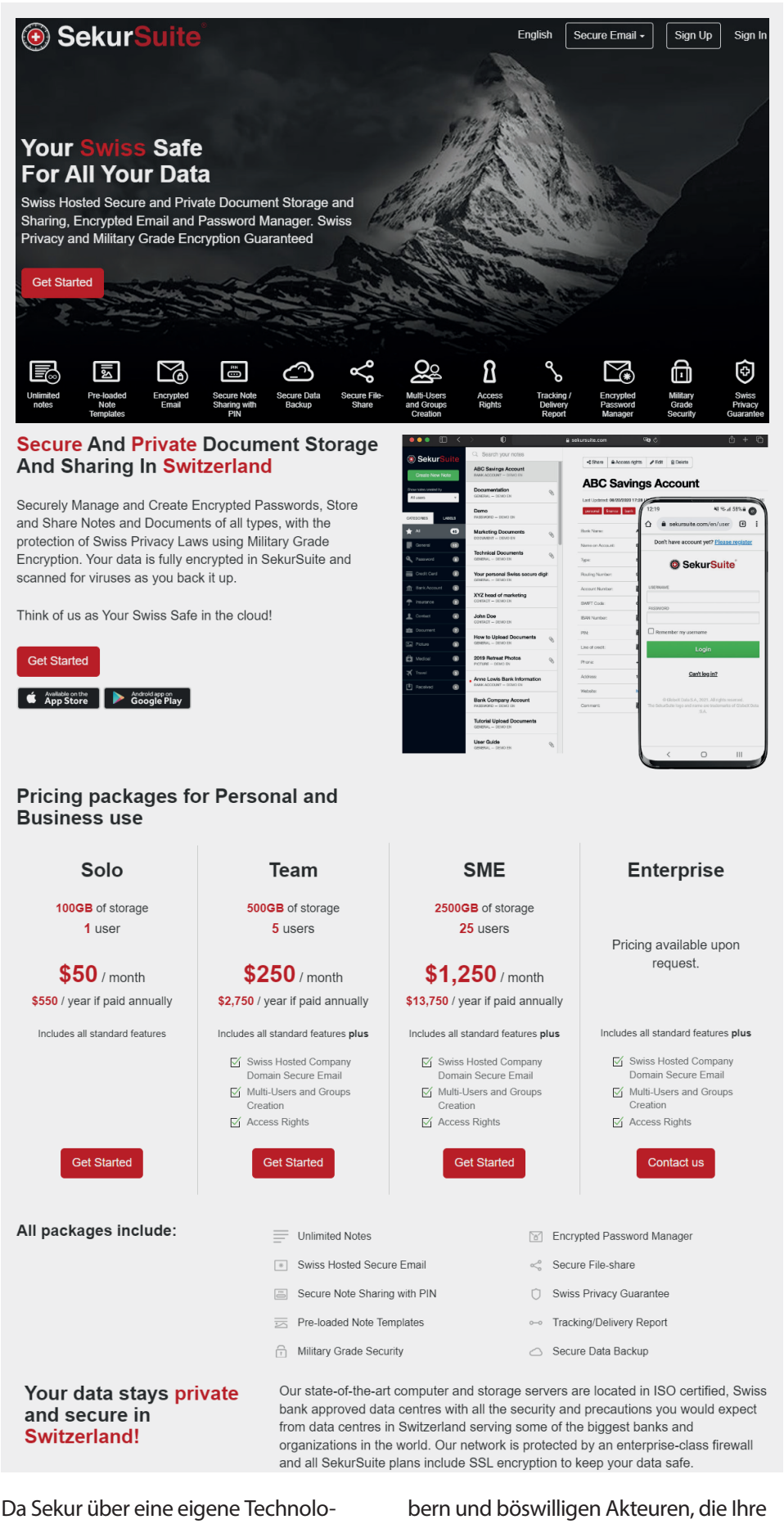
SekurSuite

SekurSuite ist eine in der Schweiz gehostete, sichere und private Dokumentenspeicherung und -freigabe mit verschlüsselter Email und Passwortmanager. Schweizer Datenschutz und militärische Verschlüsselung garantiert!

PRIVATSPHÄRE

Die Lösungen von Sekur für Cybersicherheit und Datenschutz werden alle in der Schweiz gehostet und schützen die Daten der Benutzer vor jeglichen Anfragen von außen.

Kein USA PATRIOT Act, kein CLOUD Act, kein Cybersecurity Information Sharing Act



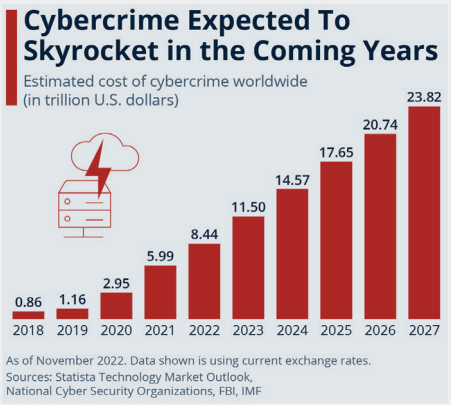
Da Sekur über eine eigene Technologie verfügt, unterliegt sie nicht den einschneidenden Gesetzen wie dem CLOUD Act. Dies gewährleistet, dass Ihre Informationen sicher sind vor Datenräubern und böswilligen Akteuren, die Ihre persönlichen Daten für kommerzielle oder kriminelle Zwecke ohne Ihr Wissen verwenden. Alle Kommunikationsdaten werden in der Schweiz gespeichert.

NEUESTE PRESSEMITTEILUNGEN

Am 2. August 2023 verkündete Sekur die Unterzeichnung eines Wiederverkäuferabkommens mit Digital Smart Solution Sarl („DSS"), einem Beratungsunternehmen für IT-Dienstleistungen mit Sitz in Casablanca, Marokko. DSS beabsichtigt, sich an die ersten und drittgrößten Telekommunikationsbetreiber in Marokko zu wenden, sowie an mehrere große Bankengruppen und Regierungsorganisationen. Grund für diesen strategischen Schritt ist die deutliche Zunahme von Cyberangriffen auf Mobiltelefone und BEC-Angriffen (Business Email Compromise) in der Region. Die ins Visier genommenen Telekommunikationsunternehmen haben zusammen mehr als 20 Millionen Mobilfunkteilnehmer, wobei über 15% dieser Teilnehmer auf Unternehmen entfallen. **Alain Ghiai, CEO von Sekur Private Data, kommentierte:** „Wir freuen uns, in das Königreich Marokko zu expandieren, da viele internationale Unternehmen ihre Afrika-Zentrale in Marokko haben. Marktforschungsergebnissen zufolge arbeiten etwa 90% der afrikanischen Unternehmen ohne Cybersicherheitsprotokolle, was sie anfällig für Cyberbedrohungen wie Hacking, Phishing und Malware-Angriffe macht. Die wirtschaftlichen Folgen der digitalen Unsicherheit sind bereits beträchtlich. Hier kommt Sekur ins Spiel, um eine private und sichere Kommunikation zu gewährleisten und Business Email Compromise (BEC) Angriffe mit unserer SekurSend-Funktion auf SekurMail zu verhindern und eine private und sichere Alternative zu datenverarbeitenden Messaging-Anwendungen mit unserem SekurMessenger und unserer einzigartigen Chat-by-Invite-Funktion anzubieten. Wir werden auch unser SekurVPN anbieten, da es eine wachsende Marktnachfrage nach VPN gibt.

Am 20. September 2023 verkündete Sekur, dass die Zahl der Neuanmeldungen für SekurVPN im Vergleich zum Vormonat um über 100% gestiegen ist: „Sekur verzeichnet einen Anstieg der Anmeldungen für seine VPN-Lösung, da Cyberattacken immer alltäglicher werden und der digitale Identitätsdiebstahl überhand nimmt. Das Unternehmen erwartet ein exponentielles Wachstum in den kommenden Monaten und Jahren für seine SekurVPN-Lösung und fügt Unternehmensfunktionen und andere Upgrades hinzu... Sekur plant, Ende Oktober oder Anfang November eine groß angelegte Kampagne für seine VPN-Lösung zu starten, während das Unternehmen den letzten Schliff für seine digitalen Anzeigen vorbereitet. Es gibt auch andere Pläne mit Reseller, um SekurVPN später in diesem Jahr zu starten. Darüber hinaus freut sich Sekur, dass der Webseitenverkehr für Sekur.com im letzten Monat um ca. 100% und in den letzten zwei Wochen um 650% gestiegen ist und eine Konversionsrate von 5% bei den Besuchen der organischen Suchseite verzeichnet wird. Das Unternehmen ist der Ansicht, dass in den kommenden 12 Monaten der Webverkehr so hoch sein wird, dass die Kosten für die Kundenakquise drastisch sinken könnten, da die organische Suche exponentiell zunimmt. Da Sekur das Marketing für kleine und mittlere Unternehmen (KMU) ausbaut, wird erwartet, dass die Ausgaben pro Kunde steigen werden, da SMBs mehrere Benutzer in ihrem Unternehmen haben. Es wird erwartet, dass die Ausgaben pro Nutzer auch steigen werden, wenn das Unternehmen seine verschlüsselten Lösungen SekurVoice für Sprachanrufe und SekurPRO, seine Videokonferenz- und vollständige private und sichere Kommunikationssuite, im ersten Quartal 2024 einführt."

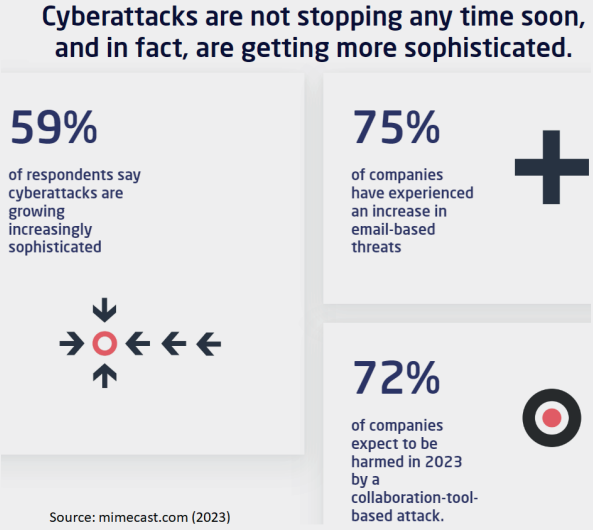
Am 14. Juni 2023 verkündete Sekur, dass seit dem Beginn der Optimierungs- und SEO-Maßnahmen im Januar 2023 die Kundenakquisitionskosten



"Nach Angaben des BR und der Tagesschau gab es Ende April Cyber-Angriffe auf 3 IT-Dienstleister des ITZ Bund, das für 200 Bundes- und Landesbehörden zuständig ist.

Bei den Angriffen seien „sehr wahrscheinlich" große Mengen an Email-Kommunikation und wohl auch personenbezogene Daten abgeflossen. Nun ist klar, warum genau die externen Dienstleister Materna, Init und adesso angegriffen wurden..."

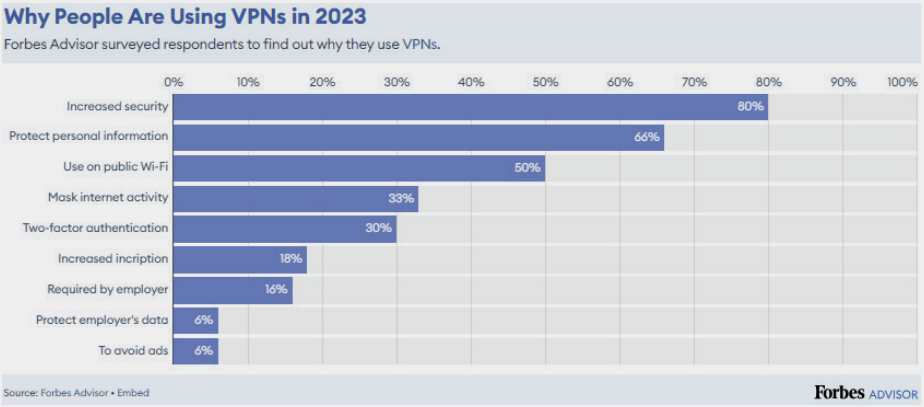
„... Dem BR oder der Tagesschau liegt wohl eine Meldung des Informationstechnikzentrums des Bundes (ITZ Bund) von Ende April mit einer Warnung vor den Angriffen vor. Darin werden die Angriffe, ihr Umfang und die Beute beschrieben. Die Cyber-Diebe sollen eine große Anzahl von Emails erbeutet haben. Wahrscheinlich sind auch persönliche Daten, Telefonnummern und Büros enthalten. Auch Informationen über laufende Projekte und teilweise ganze Email-Verläufe landeten über angehängte Dokumente bei den Angreifern." (Quelle, 2023)



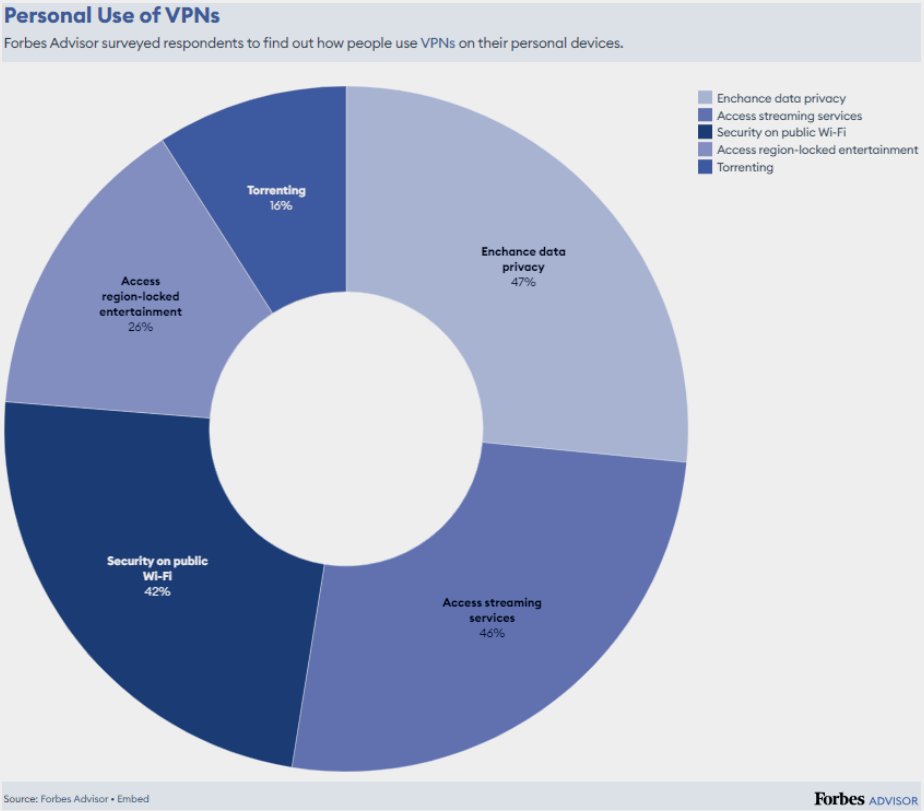
"Mit der zunehmenden Abhängigkeit der Menschen von der digitalen Technologie beim Leben, Arbeiten und Spielen ist das Risiko von Cyberangriffen erheblich gestiegen. Laut einer von Comparitech durchgeführten Studie werden jedes Jahr mehr als 71 Millionen Menschen Opfer von Internetkriminalität. Und die Zahl der Cyberangriffe nimmt von Jahr zu Jahr weiter zu... Seit dem Beginn der COVID-19-Pandemie ist die Cyberkriminalität um 300% gestiegen..."

"...Unternehmen verlieren jede Minute mehr als $17.000 USD durch Phishing. 1 % aller Datenschutzverletzungen gehen auf Malware-Infektionen zurück. Im Jahr 2021 gab es mehr als 700 Millionen Ransomware-Angriffsversuche. Kriminelles Hacking verursacht mehr als 45% der Lecks in sensiblen Daten. Malware-Angriffe kosten Unternehmen durchschnittlich $2,6 Mio. USD." (Quelle, 2023)

(„CAC“) im Juni auf $32 USD pro Kunde gesenkt werden konnten, während der Lebenszeitwert („LTV“) pro Kunde wieder gestiegen ist. Im Januar 2023 hat das Unternehmen mit der Senkung seiner Kundenakquisitionskosten („CAC“) begonnen, um sich auf gezieltes digitales Marketing, wie Google Ads und META-Kampagnen, und die Optimierung seiner Sekur-Webseite zu konzentrieren. Zuvor hatte das Unternehmen bekanntgegeben, dass es bis Ende 2023 einen CAC von $75 USD oder weniger und für 2024 einen CAC von $60 USD oder weniger aus dem Direktmarketing anstrebt, wobei B2B-Partnerschaften nicht berücksichtigt werden, was den CAC insgesamt senken würde. Das Unternehmen richtet sich derzeit an Verbraucher und KMUs und verbessert den Inhalt seiner Website, um KMUs und Besucher über die Vorteile der Datenschutz- und Sicherheitskommunikationsplattform von Sekur zu informieren. **Alain Ghiai, CEO von Sekur Private Data, kommentierte:** „Wir freuen uns sehr, dass wir unseren Plänen zur Senkung der CAC weit voraus sind. Das Unternehmen hat einen konkreten Plan, die CAC für das nächste Quartal zu optimieren und das Budget für digitales Marketing ab August 2023 schrittweise zu erhöhen. Wenn wir das Geld, das wir für digitales Marketing ausgeben, und das organische Wachstum durch die SEO-Bemühungen zusammenzählen, erreichen wir derzeit einen CAC zwischen $30 und $35 USD. Das ist eine erstaunliche Leistung in so kurzer Zeit, und ich möchte unserem gesamten Marketingteam zu seinen bisherigen Fortschritten gratulieren. Ein CAC von $75 USD oder weniger ist sehr attraktiv, da wir mit den richtigen Budgets exponentiell wachsen können, und ein CAC von unter $50 USD ist für uns außergewöhnlich, wenn wir also unter einer dieser Zahlen liegen, werden wir sehr gut abschneiden. Unsere oberste Direktive ist es, private und sichere Kommunikation für jedermann anzubieten, und da wir mit keiner Big-Tech-Plattform verbunden sind, bieten wir durch unsere proprietäre Technologie und unsere sicheren Server in der Schweiz ein wirklich unabhängiges, privates und sicheres Kommunikationsmittel ohne jegliche Datenauswertung. Wir freuen uns darauf, weiterhin allen Privatpersonen und ihren Unternehmen echten Datenschutz zu bieten und ihr geistiges Eigentum und ihre Privatsphäre vor Data Minern und bösartigen Hackern zu schützen.“

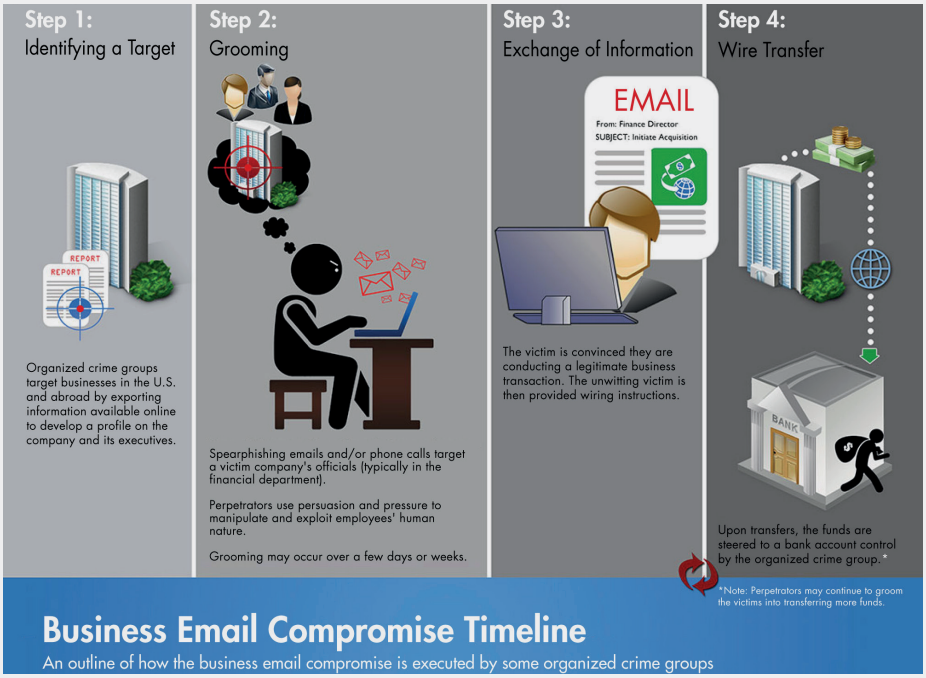


“VPNs sind nicht nur in den USA beliebt [wie die Abbildungen oben und unten zeigen]. Während zwei Drittel der befragten Internetnutzer in den USA angaben, irgendwann in ihrem Leben ein VPN zu verwenden, hat auch etwa ein Drittel der übrigen Weltbevölkerung die VPN-Nutzung übernommen... **33% aller Internetnutzer verwenden ein VPN:** Diese Zahl steigt weiter an. Studien gehen davon aus, dass der Wert des VPN-Marktes bis 2027 auf $107,5 Mrd. USD steigen wird... Kostenpflichtige VPNs bieten in der Regel mehr Funktionen und bessere Sicherheit als kostenlose... **Die durchschnittlichen Kosten für ein VPN betragen $6,50 USD pro Monat:** Die Kosten für ein VPN reichen von kostenlos bis zu etwa $13 USD pro Monat.“ (Quelle: Forbes, 2023).

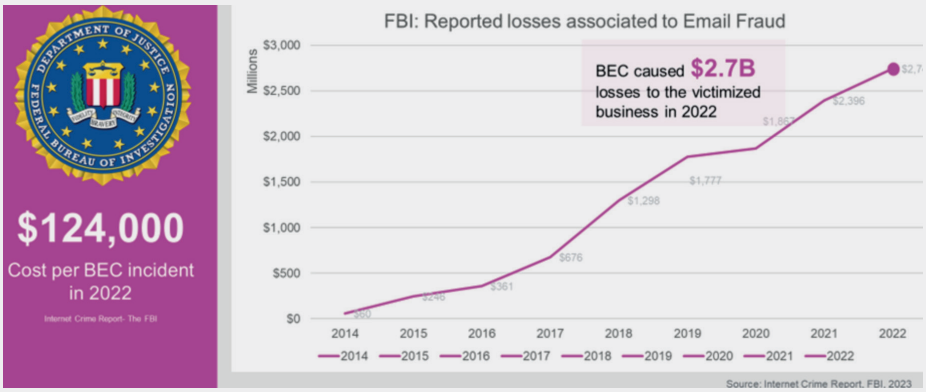


“SekurVPN nutzt seine eigene Infrastruktur und verwendet im Gegensatz zu den meisten anderen VPNs keine Hyperscaler oder Big Tech Hosting-Anbieter. Es bietet nur Schweizer IPs an, und das garantiert, dass es nur SekurVPNs eigene Server und Routing verwendet. Andere VPNs bieten Hunderte von Standorten an und verwenden Big-Tech-Provider, die die Privatsphäre der Benutzer gefährden. SekurVPN überwacht niemals die Aktivitäten der Nutzer und gibt keine Daten an Drittanbieter weiter. Da SekurVPN ein reines VPN ist, ohne gebündelte externe Dienste wie Antivirenprogramme und Werbeblocker, bleiben die Daten der Nutzer privat und werden nicht mit Drittanbietern geteilt. Mit SekurVPN muss der Nutzer seine Telefonnummer weder in der App noch im Web registrieren, was ihn für Hacker und Datenschnüffler unsichtbar macht. Sekur-Nutzer müssen keine Telefonnummer registrieren, es werden nur anonyme Schweizer IPs verwendet und es findet kein Data-Mining oder Traffic-Sharing statt... SekurVPN ist extrem einfach einzurichten und zu nutzen.“ (Quelle)

Am 6. Juni 2023 verkündete Sekur, dass die Einführung der Sekur Enterprise Solutions bis Ende Juli 2023 geplant ist. Das Angebot des Unternehmens für KMUs, große Unternehmen und Regierungsorganisationen wird eine vollständige Benutzerverwaltung, Nachrichten- und Email-Archivierungsfunktionen und ein Admin-Dashboard für Massen-Onboarding und Management von Mitarbeitern umfassen. Sekur Enterprise Solutions wird auch eine neue Email-Funktion enthalten, die in den kommenden Wochen eingeführt und angekündigt wird und es großen Organisationen ermöglicht, die Emails der C-Ebene auf dem privaten und sicheren Netzwerk von Sekur zu hosten, das die SekurSend-Funktion des Unternehmens anbietet, während der Rest der Mitarbeiter bei ihrem bestehenden Email-Hosting-Unternehmen bleibt, wodurch kostspielige Email-Migrationen vermieden werden und die Kommunikation der C-Ebene auf höchstem Niveau geschützt wird. Dieses Split-Level-Email-System ermöglicht es auch den Mitarbeitern der C-Ebene, den gleichen Firmen-Domainnamen wie der Rest der Mitarbeiter beizubehalten, während die C-Ebenen auf der SekurMail Datenschutzplattform gehostet werden. Diese Funktion ist sehr gefragt, da kleine und große Unternehmen in letzter Zeit das Ziel von Business Email Compromise (BEC) Angriffen waren. Ein BEC-Angriff ist eine Art von Cyberkriminalität, bei der böswillige Hacker Emails nutzen, um jemanden dazu zu bringen, Geld zu senden oder vertrauliche Unternehmensdaten preiszugeben. BEC-Betrügereien sind aufgrund der zunehmenden Fernarbeit auf dem Vormarsch – laut dem FBI Internet Crime Report gab es im Jahr 2021 fast 20.000 BEC-Beschwerden beim FBI. Vor allem Mitarbeiter der Führungsebene sind das Ziel von BEC-Angriffen. Diesem Artikel auf TechTarget zufolge beginnen BEC-Angriffe oft damit, dass der Angreifer eine Zielperson auf C-Level mit einer Social-Engineering-Masche dazu bringt, Malware herunterzuladen, auf einen infizierten Link zu klicken oder eine kompromittierte Website zu besuchen. Sobald das Konto des C-Level-Managers kompromittiert wurde, kann es dazu benutzt werden, einen anderen Mitarbeiter dazu zu bringen, Geld an den Angreifer zu schicken. Eine beliebte BEC-Strategie besteht darin, eine offiziell aussehende Email an jemanden in der Finanzabteilung des Unternehmens zu senden. In der Regel wird in einer solchen Email angegeben, dass es sich um eine zeitkritische, vertrauliche Angelegenheit handelt, die eine schnellstmögliche Überweisung auf das Bankkonto eines Kunden, Partners oder

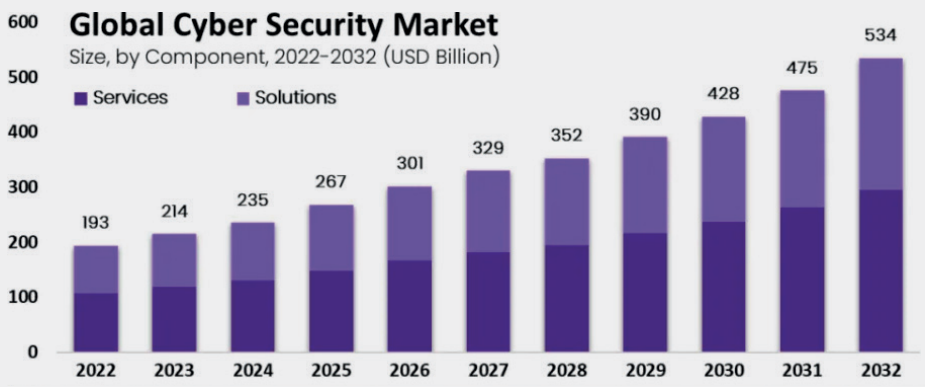


"Die Kompromittierung von Geschäfts-Emails (BEC) – auch bekannt als Kompromittierung von Email-Konten (EAC) – ist eine der finanziell schädlichsten Online-Kriminalitätsformen. Dabei wird die Tatsache ausgenutzt, dass so viele von uns bei der Abwicklung von Geschäften – sowohl privat als auch beruflich – auf Emails angewiesen sind. Bei einem BEC-Betrug senden Kriminelle eine Email-Nachricht, die scheinbar von einer bekannten Quelle stammt und eine legitime Anfrage enthält." (Quelle)



Die $2,7 Mrd. USD bedeuten einen Anstieg der Verluste durch BEC-Angriffe um 12,5% in nur einem Jahr in den USA. (Quelle: FBI 2022 Internet Crime Report) „Der BEC-Betrug hat sich weiterentwickelt und zielt auf kleine lokale Unternehmen bis hin zu größeren Firmen und persönlichen Transaktionen ab. Zwischen Dezember 2021 und Dezember 2022 gab es einen 17%-Anstieg der identifizierten globalen Verluste." (Quelle: FBI, 2023) Laut den neuesten Daten von Perception Point wurde ein Anstieg der Prävalenz von Business Email Compromise (BEC)-Angriffen um 20% sowie ein Anstieg der Phishing-Angriffe um 41% zwischen H2 2022 und H1 2023 festgestellt: „Darüber hinaus beobachtete der Bericht eine 75%-Zunahme der Angriffe auf Cloud-Collaboration-Apps und -Speicher, einschließlich Microsoft 365-Apps, Salesforce, Slack, AWS S3 Buckets und andere... Die Gesamtzahl der Cyberangriffe stieg in H1 2023 um 36%. Emails waren weiterhin der Hauptvektor für die Verbreitung bösartiger Inhalte, wobei in der ersten Hälfte des Jahres 2023 eine von 100 versendeten Emails als bösartig eingestuft wurde... Wir gehen davon aus, dass Cyberkriminelle ihre Werkzeuge weiter schärfen werden, um ein breiteres Spektrum an Kommunikations- und Kollaborationskanälen ins Visier zu nehmen, was im Jahr 2023 wahrscheinlich zu einem noch nie dagewesenen Anstieg der Angriffe führen wird. Unternehmen sollten proaktive Sicherheitsmaßnahmen ergreifen und auf neue Technologien und ganzheitliche, verwaltete Dienste zurückgreifen, um ihre Fähigkeit zu stärken, solche schädlichen Cyberbedrohungen zu verhindern und zu beseitigen."

Partners der Lieferkette erfordert. Der Angreifer hofft, dass die ahnungslose Person in der Finanzabteilung denkt, dass sie ihrem Unternehmen hilft, indem sie einen schnellen Geldtransfer ermöglicht – in Wirklichkeit schickt sie aber Geld auf das Bankkonto des Angreifers. **Die Unternehmenslösungen von Sekur werden sich preislich von den Consumer-Versionen unterscheiden:** SekurMail kostet $10 USD/Monat/Benutzer, mit Alias-Emails $7 USD/Monat/Alias, SekurMessenger $9 USD/Monat/Benutzer und SekurVPN $9 USD/Monat/Benutzer. Neue Lösungen wie SekurVoice und SekurPro werden verschlüsselte Sprach- und Videoübertragungen in das Angebot aufnehmen und sind für $20 USD/Monat/Benutzer bzw. $25 USD/Monat/Benutzer geplant. Der Jahrespreis wird 11-mal monatlich sein, um einen kostenlosen Monat des Dienstes anzubieten. Unternehmen werden wie heute in der Lage sein, für jede Lösung individuelle Pakete zu schnüren. Kunden können nun einfach auf die Sekur-Webseite gehen und entweder SekurMail, SekurVPN oder SekurMessenger auswählen und ein beliebiges Add-on für eine oder beide der anderen beiden Lösungen wählen, die nicht als primäre Wahl ausgewählt wurden. Add-ons werden mit einem Rabatt angeboten, wenn sie mit einer einzigen Lösung gebündelt werden. Das Unternehmen sieht bereits die Vorteile des Angebots der Add-ons, da mehr als 50% der Kunden sich für die Bündelung von Lösungen entscheiden. **Alain Ghiai, CEO von Sekur Private Data, kommentierte:** „Wir freuen uns sehr, dass wir auf dem besten Weg sind, unsere Sekur Enterprise Solutions auf den Markt zu bringen, die unsere bestehenden Business Solutions verbessern und mehr Funktionen für größere Unternehmen und Regierungsorganisationen bieten werden. Wir haben eine hohe Nachfrage in Lateinamerika für diese Funktionen und wir werden für den US-Markt bereit sein, wenn wir unsere B2B-Plattform in Q4 2023 starten. Das Angebot von SMB- und Enterprise-Lösungen ist Teil der Kernstrategie des Unternehmens ab dem vierten Quartal 2023, da diese Lösungen unsere durchschnittlichen Ausgaben pro Kunde erhöhen und eine stabilere und festere Kundenbasis schaffen, während wir gleichzeitig den riesigen Verbrauchermarkt bedienen. Allein in den USA gibt es über 30 Millionen Kleinunternehmen, und wir planen, einen Teil dieser Unternehmen zu schützen, beispielsweise vor BEC-Angriffen. Da wir nicht an eine Big-Tech-Cloud-Plattform angeschlossen sind, bieten wir mit unserer proprietären Technologie und unseren sicheren Servern in der Schweiz ein wirklich unabhängiges, privates und sicheres Kommunikationsmittel ohne Data-Mining. Wir freuen uns darauf, weiterhin allen Privatpersonen und ihren Unternehmen echten Datenschutz zu bieten und ihr geistiges Eigentum und ihre Privatsphäre vor Data-Minern und bösartigen Hackern zu schützen."



Der Markt für Cybersicherheits- und Datenschutzlösungen ist in den letzten Jahren schnell gewachsen und wird voraussichtlich auch in absehbarer Zukunft weiter expandieren. Dieses Wachstum wird in erster Linie durch die zunehmende Häufigkeit und Raffinesse von Cyberbedrohungen sowie die wachsende Abhängigkeit von Unternehmen, Regierungen und Privatpersonen von der digitalen Technologie angetrieben. Laut Fortune Business Insights wird der weltweite Markt für Datenschutzsoftware bis zum Jahr 2029 voraussichtlich $25,85 Mrd. USD erreichen, bei einer CAGR von 40,8% im Prognosezeitraum 2022-2029: „Nordamerika wird voraussichtlich den größten Marktanteil halten... Die zunehmende Besorgnis über Verletzungen des Schutzes persönlicher und vertraulicher Daten veranlasst Unternehmen zur Einführung von Datenschutzsoftware... Die wachsende Sorge um den Datenschutz hat die Regierungen verschiedener Länder gezwungen, Gesetze und Vorschriften zur Durchsetzung des Datenschutzes einzuführen... Da die Zahl der IoT-Geräte und -Anwendungen weiter zunimmt, wird erwartet, dass auch der Markt für Datenschutzmanagement-Anwendungen wachsen wird, was in den kommenden Jahren zu einer erheblichen Expansion der Branche führen wird."

Am 25. Mai 2023 verkündete Sekur seine Finanzergebnisse für das erste Quartal 2023, mit einer Umsatzsteigerung von 50% im Vergleich zum ersten Quartal 2022. Alain Ghiai, CEO von Sekur Private Data, kommentierte: „Wir freuen uns, unseren Aktionären zeigen zu können, dass unser Plan, den Umsatz zu steigern und gleichzeitig die Kosten zu senken, aufgeht. Der Umsatz stieg im ersten Quartal 2023 um 50% gegenüber dem ersten Quartal 2022, die Kosten sanken im ersten Quartal 2023 um 55% gegenüber dem ersten Quartal 2022 und wir schlossen das erste Quartal 2023 mit einer soliden Bilanz ab. Wir beabsichtigen, unseren Plan für 2023 fortzusetzen, der darin besteht, unsere Lösungen zu verbessern, unsere Kundenakquisitionskosten („CAC") zu senken und unsere Budgets für digitales Marketing proportional zu erhöhen, da die CAC sinken. Unsere CAC sinken gemäß unserer jüngsten Pressemitteilung vom 9. Mai 2023, und wir arbeiten weiter daran, sie zu senken. Wir haben bisher großartige Ergebnisse erzielt und in einigen Kampagnen unsere CAC auf bis zu $28 USD gesenkt. Der Plan sieht vor, das digitale Marketing zu verstärken, während wir unsere CAC senken, und von dort aus aufzustocken. Wir erwarten für 2023 einen Umsatzanstieg gegenüber 2022, dank eines niedrigeren CAC und der Einführung neuer Lösungen sowie verschiedener Verbesserungen an unseren bestehenden Lösungen. Wir möchten uns auch bei all unseren Aktionären für ihre Unterstützung bedanken und freuen uns darauf, noch bessere Finanzergebnisse für 2023 zu präsentieren."

Am 16. März 2023 verkündete Sekur, dass das Unternehmen vom Silicon Review Magazine in die Liste der „5 besten Unternehmen für Cybersicherheit im Jahr 2023" aufgenommen wurde. Der Artikel kann hier eingesehen werden..."

NEUESTE INTERVIEWS

Gestern wurden Alain Ghiai, CEO von Sekur, von Rich TV Live interviewt.

Alain sprach mit Roman Balmakov von The Epoch Times´ Facts Matter über die Bedeutung der Schweizer Privatsphäre.

Alain wird regelmäßig im Rahmen der Serie „Hack of the Week" auf NewToTheStreet.com interviewt.

Vor kurzem wurde Alain von dem renommierten Cybercrime Magazine interviewt.

Im Juni sprach Alain im The Street Podcast über die gesunkenen Kundenakquisitionskosten und die globale Vision des Unternehmens.

NEUESTE ARTIKEL

Die 15 Artikel, die im Jahr 2023 über Sekur veröffentlicht wurden, haben bis heute 215.650 Seitenaufrufe auf Benzinga erreicht.

Weitere ausgewählte Artikel:

"Sekur: Safeguarding Your Digital World" (Zimtu Capital, September 2023)

"Redefining Digital Security: The Rise of Sekur Private Data Ltd." (Tech Times, August 2023)

"Securing Your Digital Footprints: Sekur Private Data Ltd. Charts the Future" (Hackermoon, August 2023)

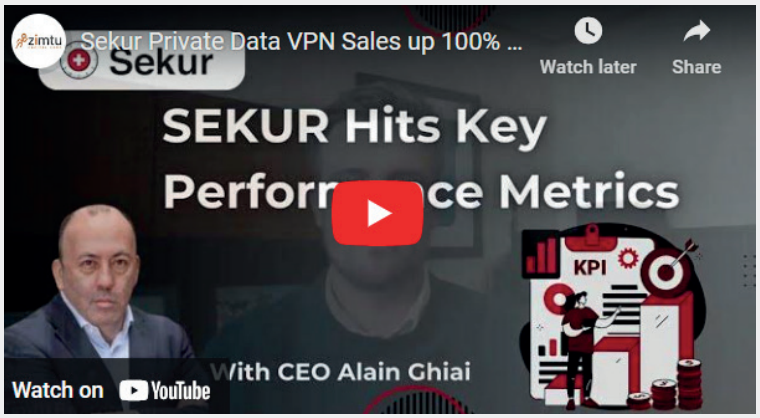
"Sekur Private Data Ltd.: Bridging the Gap between Privacy and Technology" (Next Gen Hero, August 2023)

"Reshaping Digital Privacy: Sekur's Solution to Cybersecurity Threats" (Daily Caller, April 2023)

Klicken Sie auf den Player hierüber oder hier, um das Video-Interview anzusehen.

Klicken Sie auf den Player hierüber oder hier, um das Video-Interview anzusehen.

Klicken Sie auf den Player hierüber oder hier, um das Video-Interview anzusehen.



Klicken Sie auf den Player hierüber oder hier, um das Video-Interview anzusehen.

MANAGEMENT & AUFSICHTSRAT

ALAIN GHIAI
Gründer, Präsident, CEO, Direktor

Alain gründete Sekur Private Data Ltd. und ist seit März 2017 CEO und Direktor. Seit Juni 2018 ist er als Präsident und Corporate Secretary des Unternehmens tätig. Alain gründete auch **GlobeX Data S.A.** („GDSA") und ist seit 2007 als CEO und Direktor des Unternehmens tätig. Er gründete auch **GlobeX Data Inc.** („GlobeX US") und ist seit 2012 als CEO und Direktor tätig. Alain besuchte das California College of Arts in San Francisco, wo er 1994 seinen Bachelor of Architecture erwarb. Alain verfügt über mehr als 15 Jahre Erfahrung in der Softwarebranche und war maßgeblich an der Entwicklung des Unternehmens und seiner Börsennotierung im Jahr 2019 beteiligt.

SCOTT DAVIS
CFO

Scott ist ein Chartered Professional Accountant und Partner von **Cross Davis & Company LLP,** einem Unternehmen, das sich auf die Bereitstellung von Buchhaltungs- und Managementdienstleistungen für börsennotierte Unternehmen konzentriert. Zu seinen Erfahrungen gehören CFO-Positionen bei mehreren an der TSX Venture Exchange notierten Unternehmen und er war in der Vergangenheit in leitenden Positionen tätig, darunter 4 Jahre bei **Appleby Global Group Services Ltd.** als Assistant Financial Controller. Davor war er 2 Jahre bei **Davison & Company LLP** als Wirtschaftsprüfer, 5 Jahre bei **Pacific Opportunity Capital Ltd.** als Accounting Manager und 2 Jahre bei **Jacobson Soda & Hosak** tätig. Scott erwarb seinen CPA, CGA im Jahr 2003. Scott ist seit über 8 Jahren als Dienstleister für Technologieunternehmen tätig. Er arbeitet Seite an Seite mit Alain an der Verwaltung der Finanzen von Sekur Private Data Ltd.

HENRY SJÖMAN
Direktor

Henry ist seit 1991 als Unternehmer und Angel-Investor tätig. Er ist seit 1974 in der Elektronik- und Telekommunikationsbranche tätig und hat über sein weltweites Produktionsnetzwerk einen Großteil aller Blackberry- und Nokia-Telefone hergestellt. Henry war 1991 Mitbegründer von **Elcoteq SE**, einem Unternehmen der Elektronikindustrie, das bis 2010 an der Euro-NASDAQ notiert war. Seinen Bachelor of Science in Telekommunikation erhielt er 1974 vom Kopings Tekniska Institut (Schweden). Henry ist Direktor von Sekur Private Data Ltd. und Mitglied des Prüfungsausschusses des Unternehmens.

AMIR ASSAR
Direktor

Amir hat über 27 Jahre Erfahrung im Technologievertrieb und in der Unternehmensführung und ist derzeit AVP Sales bei **Workday Inc. (NASDAQ: WDAT)**, einem der weltweit führenden Softwareunternehmen. Bevor er zu Workday kam, war Amir eine der wichtigsten Führungskräfte bei **Adaptive Insights**, wo er maßgeblich daran beteiligt war, das Unternehmen als Marktführer im Bereich Finanzdatenanalyse zu etablieren, was in einem Börsengang im Juni 2018 und der Übernahme durch Workday für $1,55 Mrd. USD im August 2018 gipfelte. Amir begann seine Technologiekarriere 1993 bei **Actel Corp.** als Western USA Director of Sales. Actel war ein führender Anbieter von Field Programmable Gate Arrays (FPGA) und wurde von **Microsemi Corp.** übernommen, einem in Kalifornien ansässigen Anbieter von Halbleiter- und Systemlösungen für die Luft- und Raumfahrt, Verteidigung, Kommunikation, Rechenzentren und Industriemärkte. Von dort aus arbeitete Amir für mehrere erfolgreiche aufstrebende Technologieunternehmen im Silicon Valley, darunter **Annuncio Software** (von **PeopleSoft** übernommen), **NetScaler** (von **Citrix** übernommen), **DataPower** (von **IBM** übernommen) und IBM, wo er leitende Positionen im Vertriebsmanagement und in der Geschäftsführung innehatte. Bei DataPower war er Teil des ursprünglichen Vertriebsleitungsteams, das das Unternehmen von einem jungen Start-up ohne Kunden zu einem $300-Mio.-Geschäft aufbaute und es gleichzeitig zu einer der erfolgreichsten Akquisitionen von IBM machte. Er ist verheiratet und lebt mit seiner Frau in San Francisco, Kalifornien. Amir ist Direktor von Sekur Private Data Ltd. und Mitglied der Geschäftsführung des Unternehmens.

DR. CLAUDIO ALBERTI
Direktor

Caudio ist seit 2017 CTO und Mitbegründer von **GenomSys**, einem Schweizer Unternehmen, das sich auf die Komprimierung und den Transport von genomischen Sequenzdaten spezialisiert hat. Er leistet einen wichtigen Beitrag zu MPEG-G, dem neuen ISO/IEC-Standard für die Darstellung von Genomsequenzierungsdaten, und ist derzeit Herausgeber des zweiten Teils des Projekts „Coding of Genomic Information". Nach seinem Master-Abschluss in Ingenieurwesen am Politecnico di Milano (Italien) und seinem Doktorat an der EPFL (Lausanne, Schweiz) entwarf und entwickelte er Lösungen für Unternehmen, die digitale Medien verarbeiten und Informationssicherheit anbieten. Derzeit arbeitet er an der Entwicklung von MPEG-G-kompatiblen Genomverarbeitungsanwendungen mit genomischen Kompetenzzentren wie dem Schweizerischen Institut für Bioinformatik, dem James Hutton Institute (UK) und dem Carl R. Woese Institute for Genomic Biology (University of Illinois at Urbana Champaign) zusammen.

HAFTUNGSAUSSCHLUSS UND INFORMATIONEN ZU ZUKUNFTSGERICHTETEN AUSSAGEN

Rockstone Research, Zimtu Capital Corp. („Zimtu") und Sekur Private Data Ltd. („Sekur") weisen Investoren darauf hin, dass die hierin enthaltenen zukunftsgerichteten Informationen keine Garantie für zukünftige Ergebnisse oder Leistungen darstellen und dass die tatsächlichen Ergebnisse aufgrund verschiedener Faktoren erheblich von den in den zukunftsgerichteten Informationen enthaltenen abweichen können. Der Leser wird auf die öffentlichen Unterlagen von Sekur verwiesen, um eine vollständigere Diskussion solcher Risikofaktoren und ihrer potenziellen Auswirkungen zu erhalten, die über die auf SEDAR hinterlegten Dokumente unter www.sedar.com abgerufen werden können. **Alle Aussagen in diesem Bericht, die nicht auf historischen Fakten beruhen, sind als zukunftsorientierte Aussagen zu betrachten. Ein Großteil dieses Berichts besteht aus Aussagen über Prognosen. Aussagen in diesem Bericht, die zukunftsorientiert sind, beinhalten**, dass sich Unternehmen, die Cybersicherheitsprodukte verkaufen, angesichts der zunehmenden Komplexität von Cyberbedrohungen und der immer größer werdenden Angriffsfläche in einer Position von erheblicher Relevanz und Chance befinden; dass Sekur sich durch sein außergewöhnliches Produktportfolio und einen stetig wachsenden Kundenkreis von anderen Unternehmen für Cybersicherheit und Datenschutz abhebt und dass Sekur mit innovativen Lösungen, die auf die sich entwickelnden digitalen Bedrohungen und Datenschutzbelange zugeschnitten sind, einen hervorragenden Ruf für den Schutz sensibler Informationen erworben hat, was das Unternehmen und seine Aktionäre für vielversprechende Wachstumsperspektiven in der sich ständig weiterentwickelnden Landschaft der Cybersicherheit positioniert; dass es, solange die Cyberbedrohungen bestehen und sich weiterentwickeln, eine kontinuierliche Nachfrage nach innovativen Lösungen für Cybersicherheit und Datenschutz geben wird; dass ein erhöhtes Bewusstsein die Nachfrage nach Cybersicherheitsprodukten antreibt; dass in dem Maße, in dem Regierungen und Unternehmen sicherheitsbewusster werden, Unternehmen, die Cybersicherheitsprodukte verkaufen, einen wachsenden Markt für ihr Angebot vorfinden werden; dass die Cybersicherheitsbranche mit kontinuierlicher Innovation, Anpassung an neu auftretende Bedrohungen und dem Engagement für den Schutz digitaler Ökosysteme weiterhin eine wichtige Rolle beim Schutz unserer vernetzten Welt spielen wird; dass 65 % der Unternehmen planen, ihre Ausgaben für Cybersicherheit im Jahr 2023 zu erhöhen; dass ein Anstieg der Ausgaben für Cybersicherheit im Jahr 2023 und in den Folgejahren erwartet wird; dass Cyberangriffe im Jahr 2023 in die Höhe schnellen und die Ausgaben in diesem Jahr und in den Folgejahren steigen werden; dass raffiniertere Cyberangriffe durch künstliche Intelligenz oder Geo-Phishing die Unternehmen zu höheren Ausgaben zwingen werden; dass Experten schätzen, dass die Gesamtkosten der Cyberkriminalität in diesem Jahr 8 Billionen US-Dollar erreichen werden; dass kleine und mittlere Unternehmen (KMU) im Jahr 2023 schätzungsweise 29. Es wird geschätzt, dass kleine und mittlere Unternehmen (KMU) im Jahr 2025 29,8 Mrd. US-Dollar für verwaltete Sicherheitsdienste ausgeben werden und dass sie Prognosen zufolge 90 Mrd. US-Dollar für Cybersicherheit ausgeben werden; dass ein beträchtlicher Teil der Unternehmen weltweit (73 %, um genau zu sein) plant, seine Ausgaben für Cybersicherheit im Jahr 2023 zu erhöhen; dass Google angekündigt hat, die Cybersicherheit zu stärken, indem es innerhalb von fünf Jahren mehr als 10 Mrd. US-Dollar investiert; dass die Notwendigkeit, zunehmend digitalisierte Unternehmen, Geräte des Internets der Dinge (IoT) und Verbraucher vor Cyberkriminalität zu schützen, die weltweiten Ausgaben für Cybersicherheitsprodukte und -dienstleistungen auf 1. 75 Billionen Dollar im Fünfjahreszeitraum von 2021 bis 2025 in die Höhe treiben werden; dass Cyberkriminalität die Welt bis 2025 jährlich 10,5 Billionen Dollar kosten wird; dass Cybersicherheit der einzige Posten ist, für den es theoretisch kein Ausgabenlimit gibt; dass die weltweiten Ausgaben für Cybersicherheit in diesem Jahr 219 Milliarden Dollar erreichen und in den nächsten drei Jahren auf fast 300 Milliarden Dollar ansteigen werden; dass die diesjährigen Investitionen in Cybersicherheitshardware, -software und -dienstleistungen voraussichtlich um 12. dass die Investitionen in Cybersicherheits-Hardware, -Software und -Dienstleistungen in diesem Jahr im Vergleich zu 2022 um 12,1 % steigen und das Wachstum der gesamten IT-Ausgaben übertreffen werden; dass fast alle Branchen und Unternehmensgrößen bis 2026 ein niedriges zweistelliges Wachstum verzeichnen werden; dass Analysten erwarten, dass der Cybersicherheitsmarkt sein anhaltendes Wachstum fortsetzen wird und dass zu den größten Geldgebern Organisationen im Bankwesen, in der Fertigung, bei professionellen Dienstleistungen und in Regierungen gehören werden, die in diesem Jahr mehr als ein Drittel aller Cybersicherheitsausgaben tätigen werden; dass Software, das am schnellsten wachsende Segment, in diesem Jahr 47% aller Ausgaben ausmachen wird, gefolgt von Dienstleistungen (39%) und Hardware (13%); dass Unternehmen, die Cybersicherheitsprodukte verkaufen, eine glänzende Zukunft vor sich haben; dass Unternehmen und Einzelpersonen sich zunehmend Cybersicherheitslösungen zuwenden werden, um ihre digitalen Vermögenswerte und ihre Privatsphäre zu schützen; dass mit dem Wachstum der digitalen Wirtschaft auch die digitale Kriminalität zunimmt; dass sich der Schaden durch Cyberangriffe bis 2025 auf etwa 10. 5 Billionen jährlich bis 2025 belaufen wird; dass sich das Volumen der Bedrohungen von 2021 bis 2022 fast verdoppeln wird; dass sich die Gesamtchance auf einen überwältigenden Markt von 1,5 bis 2 Billionen Dollar beläuft, und; dass das derzeitige Käuferklima einen einzigartigen Moment für Innovationen in der Cybersicherheitsbranche darstellen kann; dass die Wachstumsaussichten für Anbieter im Cybersicherheitsmarkt außerordentlich vielversprechend sind; dass die Schweiz nicht anfällig für Umweltrisiken wie Wirbelstürme, Tsunamis, Vul-

kane, Erdbeben, Waldbrände oder Überschwemmungen ist; dass Unternehmen in den nächsten fünf Jahren $1,75 Billionen für Cybersicherheit ausgeben werden; dass die Ausgaben für mobile Sicherheit bis Ende 2024 voraussichtlich 7. dass der Mangel an mobiler Sicherheit eine der am schnellsten wachsenden Bedrohungen im Bereich der Cybersicherheit sein wird; dass Unternehmen ihre Budgets für Cybersicherheit stetig erhöhen; dass, sobald die Verkäufe von Sekur in Mexiko in Schwung kommen, eine Ausweitung auf andere Länder geplant ist, in denen America Movil mit seiner Marke Claro tätig ist, wie z.B. Kolumbien, Peru und andere lateinamerikanische Länder, wenn das Geschäft in den nächsten Jahren wächst; dass Sekur in den kommenden Monaten und Jahren ein exponentielles Wachstum für seine SekurVPN-Lösung erwartet und Unternehmensfunktionen und andere Upgrades hinzufügt; dass Sekur plant, Ende Oktober oder Anfang November eine groß angelegte Kampagne für seine VPN-Lösung zu starten, während es den letzten Schliff für seine digitalen Anzeigen vorbereitet; dass es auch andere Pläne mit Wiederverkäufern gibt, um SekurVPN später in diesem Jahr zu starten; dass Sekur davon ausgeht, dass in den kommenden 12 Monaten der Web-Traffic so hoch sein wird, dass die Kosten für die Kundenakquise drastisch sinken könnten, da die organische Suche exponentiell ansteigt; dass, da Sekur das SMB-Marketing für Unternehmen verstärkt, die Ausgaben pro Kunde voraussichtlich steigen werden, da SMBs mehrere Benutzer in ihrem Unternehmen haben; dass die Ausgaben pro Benutzer ebenfalls steigen werden, da Sekur seine verschlüsselten Lösungen für Sprachanrufe SekurVoice und SekurPRO, seine Videokonferenz- und vollständige private und sichere Kommunikationssuite, im ersten Quartal 2024 einführt; dass Sekur über die notwendige physische Umgebung verfügt, um die Server 24 Stunden am Tag, sieben Tage die Woche in Betrieb zu halten, selbst im Falle von Stromausfällen und größeren Naturkatastrophen; dass die Produkte von Sekur sicherstellen, dass Ihre Informationen vor konkurrierenden Räubern oder Agenturen und Einrichtungen mit persönlichen Motiven sicher sind, die in Ihre Privatsphäre eindringen und Ihre Daten ohne Ihr Wissen stehlen würden; dass Sekur sicherstellt, dass nur der Absender und der beabsichtigte Empfänger die ausgetauschten Nachrichten lesen können; dass die Daten, die Sekur speichert, sicher sind und dass Ihre Konversationen völlig privat bleiben und von niemandem eingesehen werden können, und dass der Dienst sicher ist und von niemandem kompromittiert werden kann; dass Sekur die sicherste Umgebung für Ihre digitale Kommunikation bietet; dass Sekur das Risiko des Abfangens von Daten vom Gerät des Absenders eliminiert und dass „BEC" (Business Email Compromise) und E-Mail-Phishing-Vorfälle eliminiert werden; dass Sekur niemals die Aktivitäten der Benutzer überwacht und niemals Daten mit Drittanbietern teilt; dass Sekur durch seine eigene Technologie nicht den einschneidenden Gesetzen wie dem CLOUD Act, USA PATRIOT Act oder Cybersecurity Information Sharing Act unterliegt; dass DSS beabsichtigt, sich an den ersten und drittgrößten Telekommunikationsbetreiber in Marokko sowie an mehrere große Bankengruppen und Regierungsorganisationen zu wenden; dass Sekur eine private und sichere Kommunikation gewährleistet und Business Email Compromise („BEC") Angriffe verhindert; dass Sekur auch unser SekurVPN in Marokko anbieten wird; dass Sekur ein wirklich unabhängiges, privates und sicheres Kommunikationsmittel ohne Data Mining anbietet; dass Sekur sich darauf freut, allen marokkanischen Unternehmen und Regierungsorganisationen echten Datenschutz zu bieten und ihr geistiges Eigentum und ihre Privatsphäre vor Data Minern, böswilligen Hackern und schurkischen Agenten ausländischer Mächte zu schützen; dass Sekur einen konkreten Plan hat, die CAC für das nächste Quartal zu optimieren und das Budget für digitales Marketing ab August 2023 schrittweise zu erhöhen; dass, wenn die CAC-Zahlen von Sekur unter 50 USD liegen, das Unternehmen sehr gut abschneiden wird; dass die Unternehmenslösungen von Sekur einen anderen Preis haben werden als die Verbraucherversionen; dass neue Lösungen wie SekurVoice und SekurPro verschlüsselte Sprach- und Videodienste in den Angebotsmix einbeziehen werden und zu einem Preis von 20 USD/Monat/Benutzer bzw. 25 USD/Monat/Benutzer geplant sind; dass Sekur in Lateinamerika eine hohe Nachfrage nach diesen Funktionen hat und Sekur für den US-Markt bereit sein wird, wenn es seine B2B-Plattform im vierten Quartal 2023 einführt; dass das Angebot von SMB- und Enterprise-Lösungen Teil der Kernstrategie von Sekur ab Q4 2023 ist, da diese Lösungen die durchschnittlichen Ausgaben von Sekur pro Kunde erhöhen und eine stabilere und festere Kundenbasis schaffen, während sie gleichzeitig den riesigen Verbrauchermarkt bedienen; dass erwartet wird, dass Cyberkriminelle ihre Werkzeuge weiter schärfen werden, um eine breitere Palette von Kommunikations- und Kollaborationskanälen ins Visier zu nehmen, was wahrscheinlich zu einem beispiellosen Anstieg der Angriffe im Jahr 2023 führen wird; dass Sekur´s Plan, den Umsatz zu steigern und gleichzeitig die Kosten zu senken, in Erfüllung geht; dass der Plan von Sekur darin besteht, das digitale Marketing zu verstärken, während wir unsere CAC senken und von dort aus skalieren; dass Sekur für 2023 im Vergleich zu 2022 einen höheren Umsatz erwartet, dank einer niedrigeren CAC und der Einführung neuer Lösungen und verschiedener Verbesserungen; dass Sekur sich darauf freut, noch bessere Finanzergebnisse für 2023 zu präsentieren; dass der Markt für Cybersicherheits- und Datenschutzlösungen in absehbarer Zukunft weiter expandieren wird; dass die Größe des globalen Marktes für Datenschutzsoftware bis 2029 voraussichtlich $25,85 Milliarden USD bis 2029 erreichen wird, mit einer CAGR von 40,8% während des Prognosezeitraums 2022-2029, und dass Nordamerika voraussichtlich den größten Marktanteil halten wird; dass erwartet wird, dass der Markt für Datenschutzmanagementanwendungen wachsen wird, was zu einer erheblichen Expansion in der Branche in den kommenden Jahren führen wird. **Solche Aussagen beinhalten bekannte und unbekannte Risiken, Ungewissheiten und ande-**

re Faktoren, die dazu führen können, dass die tatsächlichen Ergebnisse oder Ereignisse wesentlich von denen abweichen, die in diesen zukunftsgerichteten Aussagen erwartet werden. Es kann nicht garantiert werden, dass sich solche Aussagen als zutreffend erweisen, da die tatsächlichen Ergebnisse und zukünftigen Ereignisse erheblich von denen abweichen können, die in solchen Aussagen erwartet werden. Zu den Risiken und Unwägbarkeiten gehören: Der Erhalt aller erforderlichen Genehmigungen und Erlaubnisse für die Ausübung der Geschäftstätigkeit; Ungewissheit über künftige Investitionsausgaben und andere Kosten; Finanzierung und zusätzlicher Kapitalbedarf für die Aufrechterhaltung oder Ausweitung der Geschäftstätigkeit sind möglicherweise nicht zu angemessenen Kosten oder überhaupt nicht verfügbar; legislative, politische, soziale oder wirtschaftliche Entwicklungen in den Rechtsordnungen, in denen Sekur Geschäfte tätigt, können den Fortschritt oder die Geschäftstätigkeit behindern; Betriebliche oder technische Schwierigkeiten oder Kostensteigerungen im Zusammenhang mit bestehenden Produkten oder in der Entwicklung befindlichen Produkten; die Fähigkeit, wichtige Mitarbeiter und den Betrieb zu finanzieren; Aktienkurse von Sekur und anderen Unternehmen können aufgrund vieler Faktoren fallen, einschließlich der hier aufgeführten und anderer Faktoren, die in den Veröffentlichungen der Unternehmen und anderer Unternehmen im Bereich Cybersicherheit und Datenschutz aufgeführt sind; und die Verkaufspreise der angebotenen Produkte reichen möglicherweise nicht aus, um wirtschaftlich zu bestehen; die versprochenen Produkteigenschaften können sich als falsch, unsicher/unsicher erweisen und die Benutzer können Datenverletzungen oder andere Arten von Cyberangriffen erleben; die Sicherheitsfunktionen können sich als unsicher erweisen, in welchen Fällen Sekur mit Rechtsstreitigkeiten oder anderen Arten von rechtlichen Herausforderungen konfrontiert werden kann; die Regulierungsbehörden können die Benutzer daran hindern, die Produkte von Sekur zu verwenden; die Gesetze in der Schweiz oder anderswo können sich zum Nachteil der Geschäftstätigkeit von Sekur ändern; dass die Benutzer die Produkte von Sekur als nicht nützlich erachten und den Dienst einstellen; dass Sekur keine neuen Benutzer findet, um den Betrieb aufrechtzuerhalten; dass Sekur keine Gewinne erwirtschaftet und in Konkurs geht oder seine Aktien von der Börse nimmt und dass die Investoren ihre gesamte Investition in Sekur verlieren; dass der Aktienkurs von Sekur dramatisch fällt oder die Aktien für eine lange Zeit gestoppt werden, d.h. dass die Investoren ihre Aktien nicht mehr handeln können. Das Fortbestehen von Sekur hängt davon ab, ob das Unternehmen in der Lage ist, positive Cashflows zu generieren und/oder zusätzliche Finanzmittel zu erhalten, um die laufenden Aktivitäten und Akquisitionen zu finanzieren. Laut Sekur: „Während wir weiterhin unsere Geschäftstätigkeit überprüfen, um Strategien und Taktiken zur Steigerung der Einnahmequellen und Finanzierungsmöglichkeiten zu identifizieren, gibt es keine Garantie, dass wir bei diesen Bemühungen erfolgreich sein werden; wenn wir nicht erfolgreich sind, könnten wir gezwungen sein, unsere Geschäftstätigkeit erheblich zu reduzieren oder einzuschränken, oder nicht länger als Unternehmen zu operieren. Es ist auch möglich, dass die Betriebsausgaben steigen, um das Geschäft auszubauen. Wenn wir nicht beginnen, Einnahmen zu generieren und diese deutlich zu erhöhen, um diese erhöhten Betriebskosten zu decken und/oder eine Finanzierung zu erhalten, bis unsere Einnahmen diese Betriebskosten decken, könnten unsere Geschäftstätigkeit, unsere Finanzlage und unsere Betriebsergebnisse erheblich beeinträchtigt werden. Wir können nicht sicher sein, wann oder ob wir jemals die Rentabilität erreichen werden, und wenn dies der Fall ist, sind wir möglicherweise nicht in der Lage, diese Rentabilität aufrechtzuerhalten oder zu steigern. Zu den wichtigen Risikofaktoren, die dazu führen könnten, dass die tatsächlichen Ergebnisse und die Finanzlage des Unternehmens erheblich von den in den zukunftsgerichteten Aussagen genannten abweichen, gehören unter anderem die folgenden: Spekulationscharakter des Investitionsrisikos; Betriebsverluste in der Vergangenheit; Risiko der Unternehmensfortführung; Abhängigkeit des Unternehmens von Wiederverkäufern und anderen Vertriebskanälen für den Verkauf seiner Produkte; Abhängigkeit von großen Vertriebspartnern; Abhängigkeit von Schlüsselpersonal; Abhängigkeit von Dritten; Softwarefehler; Wettbewerb; Sicherheitsbedrohungen; Forschung und Entwicklung; Verpflichtungen; Veralterung; Wachstum; Verwässerung; nicht ausgegebenes Aktienkapital; Liquiditäts- und zukünftiges Finanzierungsrisiko; Marktrisiko für Wertpapiere; und erhöhte Kosten als börsennotiertes Unternehmen. Obwohl die Geschäftsführung der Ansicht ist, dass die oben genannten Risiken alle wesentlichen Risiken, denen das Unternehmen ausgesetzt ist, angemessen und verständlich darstellen, umfassen die oben genannten Risiken nicht notwendigerweise alle Risiken, denen das Unternehmen potenziell ausgesetzt ist, da es unmöglich ist, alle möglichen Risiken vorherzusehen. Obwohl die Verwaltungsratsmitglieder versuchen werden, die Auswirkungen der Risikofaktoren zu minimieren, sollte eine Anlage in die Gesellschaft nur von Anlegern getätigt werden, die in der Lage sind, einen Totalverlust ihrer Anlage zu verkraften. Den Anlegern wird dringend empfohlen, sich vor einer Anlageentscheidung von einer Person beraten zu lassen, die auf Anlagen dieser Art spezialisiert ist. Alle zukunftsgerichteten Informationen in dieser MD&A beruhen auf den Schlussfolgerungen der Unternehmensleitung. Das Unternehmen weist darauf hin, dass die tatsächlichen Ereignisse aufgrund von Risiken und Ungewissheiten erheblich von den derzeitigen Erwartungen abweichen können. In Bezug auf die Geschäftstätigkeit des Unternehmens können die tatsächlichen Ereignisse aufgrund wirtschaftlicher Bedingungen, neuer Möglichkeiten, veränderter Budgetprioritäten des Unternehmens und anderer Faktoren von den aktuellen Erwartungen abweichen.“ Weitere Einzelheiten zu den Risikofaktoren und Unwägbarkeiten finden Sie unter www.sedar.com und in den „Management´s Discussion & Analysis“-Formularen zu-

sammen mit den Finanzberichten. **Dementsprechend sollten sich die Leser nicht in unangemessener Weise auf zukunftsgerichtete Informationen verlassen.** Rockstone und der Autor dieses Berichts sind nicht verpflichtet, die in diesem Bericht gemachten Aussagen zu aktualisieren, es sei denn, dies ist gesetzlich vorgeschrieben.

OFFENLEGUNG VON INTERESSEN UND VORSICHTSHINWEISEN

Dieser Bericht ist nicht als Aufforderung zum Kauf oder Verkauf der genannten Wertpapiere zu verstehen. Rockstone, seine Eigentümer und der Autor dieses Berichts sind keine registrierten Broker-Dealer oder Finanzberater. Bevor Sie in Wertpapiere investieren, sollten Sie Ihren Finanzberater und einen eingetragenen Makler/Händler konsultieren. Tätigen Sie niemals eine Investition allein auf der Grundlage dessen, was Sie in einem Online- oder gedruckten Bericht, einschließlich des Berichts von Rockstone, gelesen haben, insbesondere dann nicht, wenn die Investition ein kleines, wenig gehandeltes Unternehmen betrifft, das nicht sehr bekannt ist. **Der Autor dieses Berichts, Stephan Bogner, wird von Zimtu Capital, einer an der TSX Venture Exchange notierten Investmentgesellschaft, bezahlt.** Zu den Aufgaben des Autors bei Zimtu Capital gehört die Recherche und Berichterstattung über Unternehmen, an denen Zimtu Capital beteiligt ist. Der Autor dieses Berichts wird also nicht direkt von Sekur Private Data Ltd. („Sekur") bezahlt wird, profitiert der Arbeitgeber des Autors, Zimtu Capital, von der Wertsteigerung der Sekur-Aktien. Der Autor besitzt derzeit keine Aktien von Sekur, aber er besitzt Aktien von Zimtu Capital Corp. und profitiert daher von Volumen- und Kurssteigerungen der Aktie. Sekur bezahlt Zimtu für die Bereitstellung dieses Berichts und anderer Dienstleistungen zur Information der Anleger. In der Pressemitteilung vom 31. August 2023 heißt es: „Zimtu Capital Corp. (TSXv: ZC; FSE: ZCT1) (das „Unternehmen" oder „Zimtu") gibt bekannt, dass es eine Vereinbarung mit Sekur Private Data Ltd. („Sekur") unterzeichnet hat, um bestimmte Dienstleistungen aus seinem ZimtuADVANTAGE-Programm (https://www.zimtu.com/zimtu-advantage/) zu erbringen. Zimtu erhält von Sekur 50.000 Dollar für die Dauer des 3-monatigen Vertrages". Beachten Sie auch, dass die erwähnten Videointerviews und Artikel von Sekur Private Data Ltd. gesponsert wurden. **Insgesamt bestehen mehrere Interessenkonflikte.** Daher sollten die in diesem Bericht enthaltenen Informationen nicht als Finanzanalyse oder Empfehlung, sondern als Werbung verstanden werden. Die Ansichten und Meinungen von Rockstone und des Autors in Bezug auf die in den Berichten vorgestellten Unternehmen sind die eigenen Ansichten des Autors und beruhen auf Informationen, die er erhalten oder in der Öffentlichkeit gefunden hat und die als zuverlässig gelten. Rockstone und der Autor haben keine unabhängige Due-Diligence-Prüfung der erhaltenen oder in der Öffentlichkeit gefundenen Informationen vorgenommen. Rockstone und der Autor dieses Berichts übernehmen keine Garantie für die Richtigkeit, Vollständigkeit oder Nützlichkeit des Inhalts dieses Berichts oder dessen Eignung für einen bestimmten Zweck. Schließlich garantieren Rockstone und der Autor nicht, dass eines der in diesem Bericht erwähnten Unternehmen die erwartete Leistung erbringt, und Vergleiche, die mit anderen Unternehmen angestellt wurden, sind möglicherweise nicht gültig oder kommen nicht zum Tragen. Bitte lesen Sie den gesamten Disclaimer sorgfältig durch. Wenn Sie nicht mit allen Punkten des Haftungsausschlusses einverstanden sind, dürfen Sie diese Website oder eine ihrer Seiten, einschließlich dieses Berichts in Form einer PDF-Datei, nicht aufrufen. Durch die Nutzung dieser Website und/oder dieses Berichts, und unabhängig davon, ob Sie den Haftungsausschluss tatsächlich gelesen haben oder nicht, wird davon ausgegangen, dass Sie ihn akzeptieren. Die bereitgestellten Informationen sind lehrreich und allgemeiner Natur. Daten, Tabellen, Zahlen und Bilder, die nicht anders gekennzeichnet oder verlinkt sind, stammen von Stockwatch.com, Sekur Private Data Ltd. und aus dem öffentlichen Bereich. Das Titelbild (abgeändert) wurde von KanawatTH erworben und lizenziert.

Autorenprofil & Kontakt

Stephan Bogner (Dipl. Kfm., FH)
Rockstone Research
8260 Stein am Rhein, Schweiz
Telefon: +41 44 5862323
Email: sb@rockstone-research.com

Stephan Bogner studierte Wirtschaftswissenschaften mit den Schwerpunkten Finanzen & Asset Management, Produktion & Operations sowie Entrepreneurship & Internationales Recht an der International School of Management (Dortmund, Deutschland), der European Business School (London, UK) und der University of Queensland (Brisbane, Australien). Bei Prof. Dr. Hans J. Bocker schloss er im Jahr 2002 seine Diplomarbeit ("Gold im makroökonomischen Kontext unter besonderer Berücksichtigung des Preisbildungsprozesses") ab. Ein Jahr später vermarktete und übersetzte er den Bestseller "Gold Wars" von Ferdinand Lips ins Deutsche. Nachdem er 5 Jahre an den Rohstoffmärkten in Dubai gearbeitet hat, lebt er nun in der Schweiz und ist Geschäftsführer der Elementum International AG, die sich auf die zollfreie Lagerung von Gold- und Silberbarren in Hochsicherheitstresoren im St. Gotthard-Bergmassiv in den Zentralalpen spezialisiert hat.

Rockstone ist auf Aktienmärkte und börsengelistete Unternehmen spezialisiert. Der Fokus ist auf die Exploration, Entwicklung und Produktion von Rohstoff-Lagerstätten ausgerichtet, wobei derzeit auch GreenTech- und Sportartikel-Unternehmen betrachtet werden. Durch Veröffentlichungen von allgemeinem geologischen Basiswissen erhalten die einzelnen Unternehmensanalysen aus der aktuellen Praxis einen Hintergrund, vor welchem ein weiteres Eigenstudium angeregt werden soll. Sämtliche Reports und Artikel werden Lesern auf dieser Webseite und mittels dem vorab erscheinenden Email-Newsletter gleichermaßen kostenlos und unverbindlich zugänglich gemacht, wobei es stets als unverbindliche Bildungsforschung anzusehen ist und sich ausschliesslich an eine über die Risiken aufgeklärte, aktienmarkterfahrene und eigenverantwortlich handelnde Leserschaft richtet.

Für weitere Informationen und Anmeldung zum kostenlosen Email-Newsletter, besuchen Sie bitte:
www.rockstone-research.com