Cyber-Schadensbericht

Stoïk 2023

stoïk

Inhaltsverzeichnis

Vorwort

„Wir sind blind gegenüber Cyber-Risiken“

In den letzten Jahren, als Ransomware-Angriffe explodierten und Unternehmen jeglicher Größe immer häufiger Schäden erlitten, hat sich die Versicherungswelt eine Frage gestellt: Ist das Risiko „Cyber“ wirklich versicherbar?

Und das aus gutem Grund: Die Komplexität der Bedrohung, ihre Entwicklungsgeschwindigkeit und ihr systemisches Potenzial lassen die Frage aufkommen, ob ein Versicherer in der Lage ist, die Schadenserwartung eines Unternehmens auf der Grundlage seines Risikoprofils zuverlässig und dauerhaft zu bestimmen.

Es war der Ehrgeiz, dieses Ziel zu erreichen, der uns vor drei Jahren dazu bewogen hat, Stoïk zu gründen. Unsere Vision: Vollumfängliches Risikomanagement durch Ergänzung unseres Versicherungsschutzes um ein hohes Maß an Cybertechnik im Bereich des Underwritings, umfangreiche Prävention und natürlich besonders starke Schadenabwicklung und Schadenmanagement.

Seitdem haben unsere Partnermakler mehrere tausend KMU mit einem Umsatz zwischen 0 und 500 Millionen Euro in Frankreich und Deutschland mit Stoïks Ansatz gegen Cyber-Risiken abgesichert. Dafür unerlässlich war unser inhouse CERT (Computer Emergency Response Team), dass sich dezidiert mit den Sicherheitsvorfällen unserer Versicherungsnehmer befasst und unermüdlich im Einsatz ist, um sie bei Cyberangriffen zu unterstützen.

Eines der Hindernisse für die Entwicklung von Cyberversicherungen in Europa ist der fehlende Austausch von Daten über die von den Versicherern verwalteten Schadensfälle. Das kommt daher, dass die überwiegende Mehrheit der Versicherer das Fachwissen für die technische Unterstützung bei Cybervorfällen auslagert.

Wir hingegen haben das Privileg, Schadensfälle von A bis Z zu verwalten und somit quantitative und qualitative Daten zu Cybervorfällen in Europa erheben zu können. Wir erachten es als überaus sinnvoll und förderlich, unser Wissen weiterzugeben, um so Schritt für Schritt unserem Ziel näher zu kommen: die Resilienz europäischer Unternehmen gegenüber Cyber-Risiken zu stärken.

Dieser Bericht bietet daher einen ersten Überblick über den Stand der Cyber-Schadensfälle bei unseren Versicherungsnehmern. Wir planen dies von nun an jährlich zu veröffentlichen und werden dabei von Jahr zu Jahr auf einen größeren Datenbestand zurückgreifen können.

Dieser Bericht soll letztlich auch dazu beitragen, unsere kollektive Blindheit vor dieser immer schneller wachsenden Bedrohung zu mildern.

Jules Veyrat
Cofounder & CEO von Stoïk

Dieser Bericht bietet einen ersten Überblick über den Stand der Cyber-Schadensfälle bei unseren Versicherungs-nehmern. Wir planen dies von nun an jährlich zu veröffentlichen und werden dabei von Jahr zu Jahr auf einen größeren Datenbestand zurückgreifen können.

Bedrohungslage 2023

„Kleine und mittlere Unternehmen sind weiterhin im Visier“

Vincent Nguyen
Direktor für Cybersicherheit bei Stoïk

Im Jahr 2023 stellten wir einen leichten Anstieg des Angriffsvolumens fest, allerdings war dieser nicht so signifikant, wie der Anstieg, den wir 2020 zu verzeichnen hatten. Die lang erwartete Explosion von Cyberangriffen nach dem Ausbruch des russisch-ukrainischen Konflikts blieb aus. Einer rein kostengetriebenen Logik folgend, greifen Cyberkriminelle weiterhin opportunistisch die anfälligsten Unternehmen und Organisationen in allen Branchen an. So bestätigte sich 2023 der in den letzten Jahren wahrgenommene Trend, dass KMU die Hauptopfer von Cyberangriffen sind.

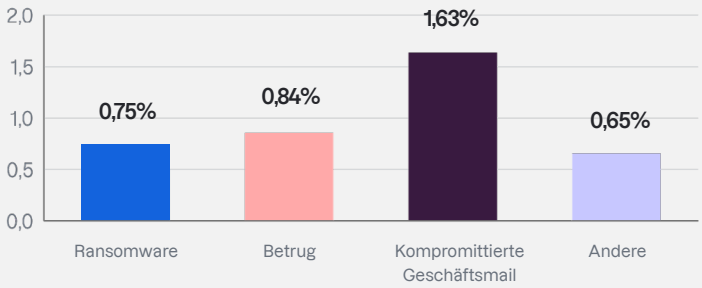
Unseren Beobachtungen zufolge sind die Schwachstellen, die Angreifer im Jahr 2023 bei mittelständischen Unternehmen ausgenutzt haben: fehlende Multifaktor-Authentifizierung, schwache Kombinationen von Benutzername und Passwort sowie nicht durchgeführte Updates. Das Fortbestehen dieser Schwachstellen ist überwiegend auf einen Mangel an Bewusstsein und Training, bereitgestelltem Budget für Cybersicherheit und Umsetzung angemessener Cybersicherheitsmaßnahmen zurückzuführen.

Auch wenn die Sensibilisierung voranschreitet, wurde das Cyber-Risiko auch 2023 noch als komplex und schwer fassbar wahrgenommen, und wenn es zu einem Vorfall kam, waren die Schäden oft groß und kostspielig.

Einer rein kostengetriebenen Logik folgend, greifen Cyberkriminelle weiterhin opportunistisch die anfälligsten Unternehmen und Organisationen in allen Branchen an.

Häufigkeit der Schadensfälle

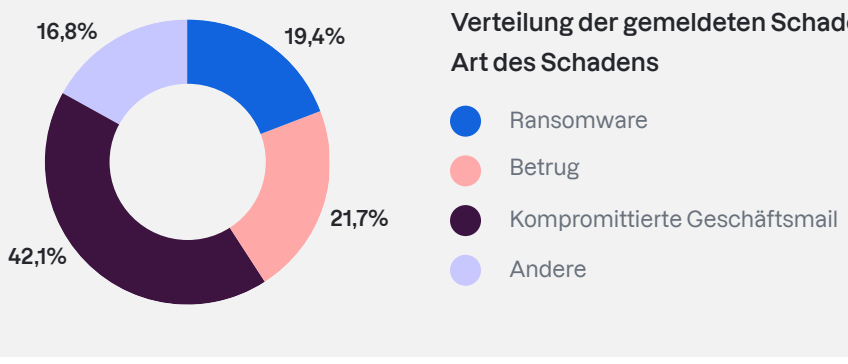
Im Jahr 2023 beobachteten wir eine Schadenshäufigkeit[1] von **3,87%** über unseren gesamten Versicherungsbestand mit folgender Kategorisierung:



Wir kategorisieren die gemeldeten Schadensfälle wie folgt:

- Wenn die Kompromittierung einer Geschäftsmail gemeldet wird, bevor eine Veruntreuung (Betrug) stattfindet oder Ransomware eingesetzt wird, wird es als **E-Mail-Kompromittierung** kategorisiert.
- Wenn ein Vorfall nach der Durchführung einer Veruntreuung (Betrug) gemeldet wird, wird es als **Betrug** kategorisiert, auch wenn der Angriffsvektor eine Kompromittierung einer Mailbox, einer Website oder eines Vermögenswerts war.
- Wenn ein Vorfall nach dem Einsatz von **Ransomware** gemeldet wird, wird es als Ransomware kategorisiert, auch wenn der Angriffsvektor eine Kompromittierung eines E-Mail-Postfachs, einer Website oder eines Vermögenswerts war.

So machen kompromittierte Mailboxen mehr als 40% unserer Schadenfälle nach Volumen aus. Doch obwohl sie nur halb so häufig auftraten, waren es Ransomware-Angriffe, die im Jahr 2023 **die größten finanziellen Auswirkungen** auf unsere versicherten Unternehmen hatten.



[1] Angabe auf der Grundlage von Schadensfällen, welche zwischen dem 1. Januar 2023 und dem 31. Dezember 2023 gemeldet wurden. Unter einem Schadensfall verstehen wir jeden von einem unserer Versicherungsnehmer gemeldeten Sicherheitsvorfall, der den Versicherungsschutz auslöst.

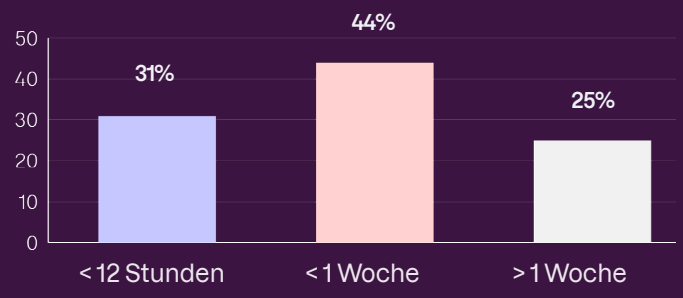
Kontrolle über die finanziellen Auswirkungen von Ransomware

Wenn die potenziellen finanziellen Auswirkungen von Ransomware den Versicherern Angst machen, dann deshalb, weil sie fast immer zu einer Betriebsunterbrechung für das Opfer führen. Nach Ablauf des zeitlichen Selbstbehalts (in der Regel zwischen 12 und 24 Stunden) verursacht jede Stunde, die vergeht, ohne dass das Informationssystem wiederhergestellt wurde, zusätzliche Kosten, welche entschädigt werden müssen. **Die Geschwindigkeit und Qualität des Einsatzes von Experten für Krisenmanagement hat einen erheblichen Einfluss auf die Höhe des Schadens.** Die ersten Stunden der Intervention sind besonders entscheidend, da sie darauf abzielen, die Ausbreitung des Angreifers innerhalb des Systems zu unterbinden und so den entstandenen Schaden zu begrenzen.

Korrelation zwischen der Dauer des Schadensfalls und der Art der Datensicherung

In 75 % der bisherigen Fälle von Ransomware konnten unsere Versicherten die Geschäftstätigkeit in weniger als einer Woche wieder aufnehmen. Alle Opfer hatten eines gemein: Die Erstellung der Datensicherungen war korrekt konfiguriert und auf Medien verfügbar, die vom Rest des Informationssystems getrennt waren. Unsere Cyber-Experten konnten das Informationssystem wiederherstellen, da die Backups vorher getestet wurden und der Backup-Katalog ebenfalls gesichert wurde. In den Fällen, in denen die Dauer eine Woche überstieg, waren die Backups des Versicherten hingegen nicht ordnungsgemäß vom restlichen IT-System getrennt worden oder nicht vor Manipulation geschützt (kein „immutable backup“).

Incident Response-Dauer bei Ransomware-Fällen



Fallstudie

Mitten im Schlussverkauf, einen Tag vor dem Wochenende, alarmierte ein E-Commerce-Unternehmen unsere Experten, dass seine Website aufgrund von Ransomware nicht verfügbar sei. Jeder Tag, an dem die Website unterbrochen war, hätte mehrere hunderttausend Euro an entgangenen Einnahmen bedeutet.

Gemeinsam mit dem CIO des versicherten Unternehmens wurden Sanierungsarbeiten durchgeführt, um die Datensicherungen wiederherzustellen und die IT-Infrastruktur vollständig neu aufzubauen. Parallel dazu machte sich ein zweites Team daran, das Informationssystem komplett neu aufzubauen, falls diese Backups sich als unbrauchbar herausstellen sollten. In nur wenigen Stunden wurde der Angreifer aus der Infrastruktur verdrängt und das Informationssystem wieder in Stand gesetzt.

Verhandlung mit Cyberkriminellen

Die Lösegeldforderungen an unsere Versicherungsnehmer beliefen sich im Jahr 2023 durchschnittlich auf rund 700.000 Euro. In der Regel lassen sich die Angreifer auf eine Verhandlung ein, die dann von unseren Teams übernommen wird. Diese Phase ist kritisch, da unsere Teams hier Zeit gewinnen können, um weiter daran zu arbeiten, das Informationssystem des Versicherten wiederherzustellen, ohne dass der Angreifer den Schaden vergrößert. Zudem reduzieren wir den geforderten Lösegeldbetrag für den Fall, dass eine Zahlung unumgänglich wird: **Im Durchschnitt haben diese Verhandlungen dazu geführt, dass die Forderungen um mehr als 53% des ursprünglichen Betrags gesenkt werden konnten.**

Der Nutzen eines externen Scans zur Verhinderung von Ransomware

In 82% der Fälle von Ransomware, die unsere Versicherungsnehmer erlitten haben, sind die Cyberkriminellen in das Informationssystem eingedrungen, indem sie sich Fernzugriffe entweder durch Brute-Force-Methoden oder nach einem erfolgreichen Phishing-Versuch verschafft haben. Nur in 18% der Fälle nutzten sie technische Schwachstellen aus.

Dass die Ausnutzung technischer Schwachstellen seltener vorkommt, liegt daran, dass alle von Stoïk versicherten Unternehmen wöchentlich gescannt und bei Auftreten einer Schwachstelle benachrichtigt werden. **So wurden durch unseren externen Scan im Jahr 2023 durchschnittlich 10 kritische Schwachstellen pro Woche in unserem Versicherungsbestand behoben.**

Bei den 18% der Fälle, in denen Schwachstellen nicht durch unseren externen Scan entdeckt wurden, handelt es sich um sogenannte Zero-Day-Schwachstellen (also noch nicht bekannte Schwachstellen) oder um Schwachstellen, die in einem Teil des Computersystems vorhanden waren, der vom Versicherten nicht explizit angegeben wurde (z. B. eine öffentliche IP-Adresse, die anhand der angegebenen Domänen oder Subdomänen nicht identifiziert werden konnte), wie es manchmal bei dem Angriff durch die Ransomware ESXiargs der Fall war - einem Angriff globalen Ausmaßes im Zusammenhang mit Tausenden von verwundbaren Servern, die im Internet exponiert waren.

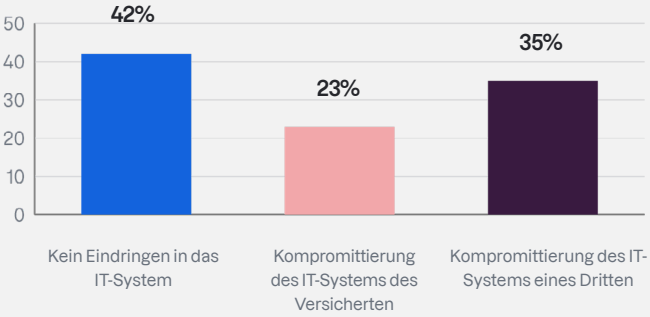
ESXiargs-Ransomware

Von Beginn an der Kampagne zur massiven Ausnutzung der ESXi-Schwachstelle synchronisierten sich unsere Experten mit dem InterCERT France, um den besten Weg zur Blockierung des Angriffs zu finden. Sie warnten daraufhin alle Versicherungsnehmer, die potenziell betroffen sein könnten, und haben so die Anzahl der erlittenen Angriffe drastisch begrenzt.

Bei den am wenigsten reaktiven Versicherten traten jedoch mehrere Fälle am selben Tag auf, aber unsere Experten konnten jedes Mal eine wirksame Entschlüsselungsmethode einsetzen und es kam zu keinen nennenswerten Schäden.

Überweisungsbetrug in all seinen Formen

Unter allen Fällen von Überweisungsbetrug, die unserem CERT gemeldet wurden, lassen sich **drei verschiedene Situationen unterscheiden:**



- In 42% der Fälle wird der Betrug **ohne Eindringen in das Computersystem** des Versicherten durchgeführt, einfach durch eine betrügerische E-Mail oder einen betrügerischen Telefonanruf von außerhalb des Unternehmens.
- In 23% der Fälle wird der Betrug **durch die Kompromittierung des Computersystems des Versicherten** durchgeführt.
- In 35% der Fälle wird der Betrug **durch die Kompromittierung des Computersystems eines Dritten** (z. B. der Buchhaltungsfirma des Versicherten) durchgeführt.

Im Jahr 2023 betrug der daraus resultierende Schaden für unsere Versicherungsnehmer durchschnittlich **47.500 €.**

Die Rechts- und Immobilienbranche, in der häufig und viel Geld überwiesen wird, war besonders bestroffen. Der Angreifer versucht meist, das Postfach einer Geschäftsmail zu kompromittieren, um dann einen günstigen Zeitpunkt abzuwarten, an dem er die IBAN des Zahlungsempfängers (z.B. die des Eigentümers einer Mietwohnung bei Immobilienmaklern) durch seine eigene ersetzt.

Auch andere Dienstleister wurden wiederholt ins Visier genommen, oft wegen kleinerer Beträge, die unbemerkt bleiben.

Fallstudie

Zwischen einem unserer Versicherten und einem seiner Lieferanten kam es zu einem Rechtsstreit: Seit mehreren Monaten bezahlte der Versicherte Rechnungen an ein Konto eines Angreifers, der sich als Lieferant ausgegeben hatte. Der Angreifer hatte die Mailbox unseres Versicherungsnehmers durch einen erfolgreichen Phishing-Angriff kompromittiert und eine schädliche Verarbeitungsregel für eingehende E-Mails hinzugefügt: Rechnungen des Lieferanten, die in der Mailbox unseres Versicherten eingingen, wurden automatisch manipuliert, wodurch die rechtmäßige IBAN durch die des Angreifers ersetzt wurde.

Die Intervention unseres CERT ermöglichte es, die Quelle der Kompromittierung zu identifizieren, die E-Mail-Postfächer unseres Versicherten zu sichern und gleichzeitig alle seine Teams für die Risiken des Finanzbetrugs zu sensibilisieren.

Wirksame Hebel zur Risikoeindämmung:

Es ist äußerst schwierig, Betrugsversuche vorherzusagen. Wenn der Angreifer auf das E-Mail-Postfach Zugriff hat, verfügt er über alle vergangenen E-Mails und kann dann z.B. mühelos eine vergangene Rechnung mit manipulierter IBAN anmahnen. Die Beibehaltung eines bestehenden Gesprächsverlaufs lassen hierbei diese Art der Betrugsversuche besonders vertrauenswürdig erscheinen.

Drei Maßnahmen, um gegen Überweisungsbetrug vorzugehen:

Einrichtung der **Multifaktor-Authentifizierung (MFA)** für E-Mail-Postfächer.

Durchführung einer **Kampagne zur Sensibilisierung** der Mitarbeiter für Phishing (Phishing-Simulation).

Einführung eines Verfahrens zur **doppelten Bestätigung von Zahlungen**, beispielsweise ab bestimmten Betragshöhen (4-Augen-Prinzip).

Sicherheit von E-Mail-Postfächern: ein beliebtes Einfallstor für Angreifer

Ein Angreifer kann eine kompromittierte Mailbox auf 3 verschiedene Weisen ausnutzen:

- **Datendiebstahl**: Der Angreifer stiehlt die Daten, die in der Mailbox gespeichert sind. Hierunter sind häufig insbesondere Dateianhänge von besonderem Interesse.
- **Veruntreuung von Geldern** durch eine Änderungen von Zahlungsinformationen (siehe obiges Beispiel).
- **Erschließung weiterer Angriffsmöglichkeiten**: Der Angreifer nutzt die kompromittierte E-Mail, um weitere Informationen oder Zugriffsrechte zu erhalten und sein Schadenspotenzial zu vergrößern. Wenn er selbst nicht dazu in der Lage ist, kann er seine Zugänge auch an Angreifer mit mehr Erfahrung weiterverkaufen.

Unsere Analyse der Schadenmeldungen im Zusammenhang mit kompromittierten E-Mail-Postfächern zeigt deutliche Unterschiede nach den von unseren Versicherungsnehmern genutzten E-Mail-Plattformen.

Häufigkeit der Postfachkompromittierung in Bezug auf genutzte E-Mail-Plattform:

x1 Google Workspace

x1,2 Microsoft Office 365

x3 Microsoft Exchange intern gehostet

Zunächst ist anzumerken, dass Nutzer von Microsoft Office 365 1,2 Mal mehr Fälle von kompromittierten E-Mail-Postfächern melden als Nutzer von Google Workspace. Dies mag zwar den Eindruck erwecken, dass Office 365-Umgebungen spezifische Schwachstellen aufweisen oder von Angreifern stärker ins Visier genommen werden als Google Workspace-Umgebungen, allerdings sollten auch andere Faktoren berücksichtigt werden wie die Popularität von Microsoft 365, die es anfälliger für Angriffe macht. Vor allem ist es entscheidend, daran zu erinnern, dass **die Sicherheit jeder E-Mail-Plattform stark davon abhängt, wie sie konfiguriert und verwaltet wird.** Die Zahlen sollten daher nicht als inhärenter Hinweis auf eine Schwachstelle in Microsoft 365 interpretiert werden.

Noch auffälliger ist, dass die Anzahl der Schadenmeldungen für kompromittierte Mailboxen bei Nutzern, die ihren eigenen Exchange-Mailserver hosten, dreimal so hoch ist wie bei Nutzern, die Google Workspace nutzen. Auch hier gilt es, keine voreiligen Schlüsse zu ziehen. Zwar erfordern die von den Versicherungsnehmern genutzten E-Mail-Umgebungen ein internes Sicherheitsmanagement und sind daher möglicherweise stärker gefährdet, wenn die Sicherheitsrichtlinien nicht strikt durchgesetzt werden, allerdings können intern gehosteten Lösungen bei guter Verwaltung ein sehr hohes Maß an Sicherheit bieten. Der Gedanke, den wir im Hinterkopf behalten sollten, ist also vor allem die Bedeutung einer sicheren Verwaltung und Konfiguration, unabhängig von der gewählten Plattform.

Aktive Versicherung zur Bewältigung von Cyberangriffen

Das Cyber-Risiko ist ein neues, unvorhersehbares, **aber antizipierbares Risiko**. Im Jahr 2023 sind immer noch zu wenige mittelständische Unternehmen auf einen Cyberangriff vorbereitet, was fatale Folgen haben kann. Um sie zu antizipieren und die Kosten von Schadensfällen zu senken, halten wir zwei Aspekte für entscheidend: die Qualität der Prävention und die Geschwindigkeit, mit der im Falle eines Angriffs reagiert werden kann.

Aktive und kontinuierliche Prävention

Das erste Ziel besteht darin, Unternehmen dabei zu helfen, die häufigsten Angriffe zu vermeiden: Dies ermöglichen wir unseren Versicherungsnehmern, indem wir ihnen die Stoïk Protect-Plattform zur Verfügung stellen. Dadurch hat der Versicherungsnehmer Zugang zu internen und externen Scans, die bekannte Schwachstellen identifizieren, bevor dies Angreifer tun, sowie zu Tools zur Sensibilisierung für Cyber-Risiken (z.B. Phishing, Betrug).

Ergänzend dazu begleiten unsere Experten die versicherten Unternehmen während der gesamten Vertragslaufzeit bei der Umsetzung von Hygienemaßnahmen zur Cybersicherheit:

- **Behebung von Schwachstellen**, die bei Scans entdeckt wurden
- Implementierung **von Multifaktor-Authentifizierung**
- Einführung einer Richtlinie für **Online- und Offline-Datensicherungen**
- Einführung einer Richtlinie für **starke Passwörter**
- Einführung einer Richtlinie zur **Verfolgung von Aktualisierungen**

Eine schnelle und effektive Möglichkeit, auf Vorfälle zu reagieren

Zweitens haben wir in diesem Bericht gesehen, dass insbesondere bei Ransomware-Vorfällen die ersten Stunden entscheidend sind, um die Kosten des Schadens zu minimieren. Aus diesem Grund **verfügen wir über ein Team von Cyber-Experten – das Stoïk-CERT – um unsere Versicherungsnehmer im Falle eines Angriffs so schnell und effizient wie möglich zu unterstützen.**

Bei Stoïk versicherte Unternehmen verfügen somit über technische und personelle Unterstützung, die es ihnen ermöglicht, in Echtzeit einen Überblick über ihren Risikograd zu erhalten und im Schadensfall von hochwertiger Unterstützung zu profitieren.

Unsere Prognose für 2024

„Angreifer werden weiterhin bekannte Schwachstellen ausnutzen“

Vincent Nguyen
Direktor für Cybersicherheit bei Stoïk

Im Jahr 2024 werden Angriffe über die Lieferkette („Supply Chain-Angriff“), in denen das Sicherheitsniveau je nach Lieferant sehr heterogen ist - man bedenke, dass das Sicherheitsniveau eines Unternehmens dem schwächsten Sicherheitsniveau seiner Anbieter entspricht - und insbesondere über Cloud-Dienste zu einem großen Risiko werden. Beide Aspekte werden in den Informationssystemen von Unternehmen immer relevanter, was die Angriffsfläche drastisch vergrößert und gleichzeitig die eigene Kontrolle stark reduziert. Dies verdeutlicht die dringende Notwendigkeit für Organisationen aller Branchen, ihre Cybersicherheit gegen diese immer raffinierteren und potenziell verheerenden Bedrohungen zu verbessern.

Angriffe auf Anbieter von Cloud-Diensten haben weitreichende Auswirkungen. Wenn einer dieser Anbieter kompromittiert wird, sind die Auswirkungen nicht auf eine einzelne Organisation beschränkt, sondern erstrecken sich auf ihr gesamtes Kundennetzwerk. Das kann bedeuten, dass **Dutzende, Hunderte oder sogar Tausende von Unternehmen die Folgen eines einzigen Angriffs zu spüren bekommen.**

Ein Beispiel aus dem Jahr 2023

Coaxis, ein Unternehmen für digitale Dienstleistungen, erlitt im Dezember 2023 einen Ransomware-Angriff, der die Hälfte aller Buchhaltungsbüros in Frankreich zum Stillstand brachte. Wenn ein IT-Dienstleister angegriffen wird, sind alle seine Kunden davon betroffen.

Gesellschaftliche und technische Trends - z.B. die Entwicklung der künstlichen Intelligenz und des IoT - scheinen sich bisher kaum auf die Cyber-Bedrohungslage auszuwirken. Wir werden jedoch vor und während der gesamten Zeit der **Olympischen und Paralympischen Spiele 2024** in Frankreich erhöhte Wachsamkeit walten lassen. Die Durchführung einer solchen Veranstaltung führt systematisch zu einer erhöhten Cyberbedrohung für alle öffentlichen und privaten Strukturen des Gastgeberlandes, und unsere Zusammenarbeit im Rahmen von InterCERT France und FIRST (Forum of Incident Response and Security Teams) wird es uns ermöglichen, schnell und effektiv darauf zu reagieren.

Die **europäische NIS-2-Richtlinie** markiert eine Revolution im Bereich der Cybersicherheit und verpflichtet eine Vielzahl von Organisationen, strenge Standards für die IT-Sicherheit und das Schadenmanagement einzuhalten. Angesichts dieser neuen Anforderungen wird die Cyberversicherung zu einem entscheidenden Instrument, nicht nur um die gesetzlichen Verpflichtungen zu erfüllen, sondern auch um finanziellen und betrieblichen Schutz vor Cyberangriffen zu bieten. Diese Veränderung führt zu einem wichtigen Wandel in der Beziehung zwischen Unternehmen und Versicherern und unterstreicht die Notwendigkeit eines tiefgreifenden Verständnisses der Cyber-Risiken und der Best Practices, um sie effektiv zu bewältigen.

stoïk

Mehr als Cyberversicherung

www.stoik.com

kontakt@stoik.com

Im Mediapark 8, 50670 Köln