CHUBB®

Risiken im Informations- und Kommunikationssektor (ICT-Sektor)

Cyberrisikobewusstsein für ICT-Unternehmen

CHUBB®

Cyberrisikobewusstsein für ICT-Unternehmen

Mitwirkende

Barry Schütte
Manager Industry Practices Benelux, Chubb

Wouter Wissink
Senior Principal Cyber Risk Engineer und Technology Industry Practitioner, Chubb

Die Cybersicherheit ist ein Risikobereich, den es zu beachten gilt. Dies gilt insbesondere, da die globalen Kosten von Cyberkriminalität im Jahr 2025 gemäss Prognosen von Cybersecurity Ventures rund 10.5 Billionen $ jährlich betragen sollen. Die ICT-Unternehmen sind Hackern dabei besonders ausgesetzt. Als Anbieter von IT-Produkten und -Dienstleistungen sind sie ein beliebtes Ziel, um Malware oder Ransomware mit einem Schlag auf zahlreiche Unternehmen zu verteilen

Die Cyberangriffe auf Kaseya und SolarWinds sind zwei bekannte Beispiele für den Schaden, den raffinierten Cyberkriminelle verursachen können. Gut organisierte Hacker werden durch die Monetarisierung ihrer Tätigkeiten immer stärker angetrieben. Ransomware stellt mittlerweile die grösste Cybergefahr dar, warnt die Agentur der Europäischen Union für Cybersicherheit.

Wenn man Cyberkriminalität Einhalt gebieten möchte, braucht es solide Sicherheitsmassnahmen sowie eine beständige Überwachung der Kontrollen. Die Risiken können stark begrenzt werden, indem man spezifische Massnahmen der IT-Hygiene ergreift. Cyberangriffe werden jedoch im Allgemeinen immer gezielter und fortschrittlicher durchgeführt. Wie sollten die ICT-Unternehmen also vorgehen, um sich selbst und andere zu schützen?

Häufige Gefahren

ICT-Unternehmen stehen zwei grundlegenden Risiken gegenüber, die miteinander verknüpft sind: Angriffe auf ihre eigenen Umgebungen und jene, die den Kunden schaden. Ein Hackerangriff auf einen Softwareentwickler oder ein Handelsunternehmen aus dem ICT-Sektor könnte zum Diebstahl vertraulicher Informationen führen, die dann wiederum von den Hackern missbraucht werden könnten, um direkt auf die Kundenumgebung zuzugreifen. Wenn ein ICT-Unternehmen einem Angriff durch eine Ransomware unterliegt, ist es eventuell nicht in der Lage, seinen Kunden wesentliche Supportdienste zu erbringen. Oder durch Backdoor-Malware beschädigte Software kann unwissentlich an Kunden verkauft werden, was so den Angriff auf Hunderte oder Tausende Unternehmen ermöglicht.

„Cyberkriminellen können auch Schaden zufügen, indem sie durch Managed Service Providers (MSPs) Zugriff auf Kunden erhalten“, warnt Wouter Wissink, Senior Principal Cyber Risk Engineer und Technology Industry Practitioner, bei Chubb.

„Die geschäftlichen und finanziellen Folgen sowie die Rufschädigung können für ICT-Unternehmen umfassend ausfallen“, erklärt Barry Schutte, Industry Practices Manager bei Chubb. „Besorgte Unternehmen müssen beispielsweise auf einen Konkurrenten zurückgreifen, was den Reingewinn beeinflusst“, erklärt er.

Schwierige Geschäftsentscheidungen

Welche Lehren kann man aus den Krisen bei Kaseya und SolarWinds ziehen? Im Fall des multinationalen US-Unternehmens Kaseya vom Juli 2021 hatten Hacker im Rahmen eines Zero-Day-Angriffs Schwachstellen in der Virtual System Administrator (VSA) Software ausgenutzt, die an MSPs und IT-Teams vertrieben wird.

Checkliste für bewährte Praktiken im Bereich der IT-Hygiene

- **Können Sie die Risiken Ihres Unternehmens und Ihrer Kunden erfassen?**
- **Wissen Sie, was zur Vermeidung dieser Gefahren zu tun ist?**
- **Gibt es robuste Massnahmen, um Cyberrisiken zu erfassen?**
- **Gibt es einen klaren Reaktionsplan im Fall eines Hackerangriffs?**

„Als ‚Man-in-the Middle' haben MSPs es mit wirklichen Cyberrisiken zu tun"

„Dieser Zwischenzeitraum ist sehr schwer zu schützen", erklärt Wissink. „Softwareunternehmen brauchen eine Woche oder länger, um solch ein Problem zu beheben. In diesem Zeitraum sind diese Entwickler stark gefährdet."

Der Schaden bei Kaseya beschränkte sich auf etwa 50 Kunden, aber bis zu 1500 nachgelagerte Unternehmen weltweit waren angeblich ebenfalls von der Ransomware betroffen.

Diese Art von Angriffen wird immer häufiger verübt. Im Jahr 2021 haben sich Zero-Day-Angriffe laut einem Bericht von Rapid7 verdoppelt. „Dies ist der kritischste Risikobereich, da er sehr schwer zu kontrollieren ist", sagt Wissink. Er hält die betroffenen Unternehmen dazu an, die Kunden unverzüglich am Tag des Hackerangriffs zu informieren, die Systeme schnell offline zu nehmen und die Kunden auf dem Laufenden zu halten.

„Dies kann für einige Unternehmen sehr schwierig sein", warnt er. „Im Grossen und Ganzen erklären Sie Ihren Kunden, dass Ihr Geschäftsmodell nicht weiter sicher ist und sie offline gehen müssen."

Hintertür-Taktiken

Sechs Monate vor dem Kaseya-Vorfall kam es zum so genannten Solarigate Supply Chain Hack, bei dem Cyberkriminelle Malware in Updates des SolarWinds Orion Softwaresystems einfügten, das bei Unternehmen zur Verwaltung von IT-Ressourcen weit verbreitet ist.

„Die Hacker verschafften sich Zugang zur Entwicklungsumgebung", erklärt Wissink. Die Malware verbreitete sich unentdeckt als reguläres Softwareupdate für die Kunden und schuf somit eine Hintertür zu ihren IT-Systemen. Rund 18.000 Kunden fielen dem Angriff zum Opfer, darunter auch US-Regierungsbehörden und globale Marken. Laut Wissink „hätten grundlegende IT-Hygienemassnahmen diesen Angriff vereiteln können".

Aufkommende Trends

Welche Trends sehen die Versicherer aktuell? Schütte zufolge verbessern die Unternehmen ihre eigenen Schutzvorkehrungen, sodass Cyberkriminelle häufiger auf Händler und Zulieferer im ICT-Sektor abzielen. Als ‚Man-in-the Middle' haben MSPs es mit wirklichen Cyberrisiken zu tun. Das stetige Wachstum in diesem Markt wurde durch einen Anstieg der Ansprüche begleitet.

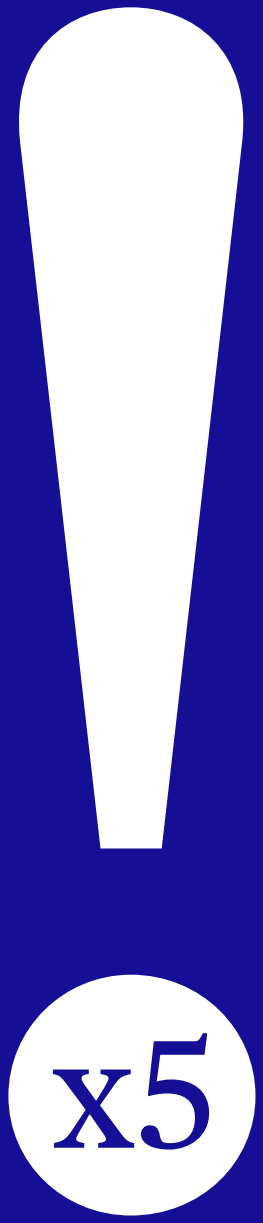
„Platform as a Service (PaaS) und Software as a Service (SaaS) sind auch stärker gefährdet", fügt er hinzu. „Das Risikoprofil hat sich umfassend erweitert, da man von Softwaresystemen vor Ort auf plattform- oder cloudbasierte Geschäftsmodelle übergegangen ist."

Die Sorgfaltspflicht ist ein weiterer aufkommender Risikobereich. „In einer Beziehung zwischen Zulieferer und Kunde wird ein ICT-Unternehmen für gewöhnlich als Experte angesehen", erklärt Schütte. „Seine Verantwortlichkeiten gehen häufig über die schriftlich dargelegten Bestimmungen eines Vertrags hinaus, wodurch die Haftungsrisiken eskalieren." Ein Anbieter riet einem Kunden dazu, zusätzliche Sicherheitsmassnahmen zu ergreifen, dokumentierte diese Beratung jedoch nicht. Als der Kunde einen Ransomware-Angriff erlebte und später vor Gericht klagte, wurde das ICT-Unternehmen für haftbar befunden.

Wie können diese Risiken nun mittels einer guten IT-Hygiene verringert werden? Wir schauen uns im Folgenden die bewährten Praktiken für ICT-Unternehmen rund um vier Schlüsselkonzepte an: Identifizieren, Vorbeugen, Erfassen und Reagieren.

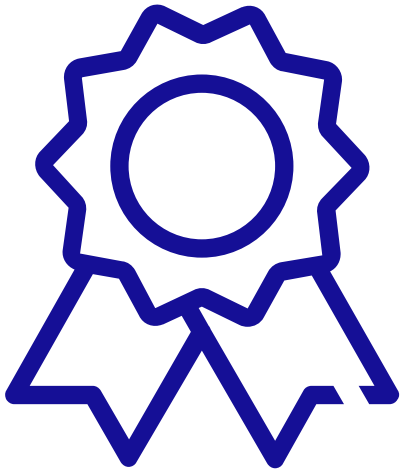
Risiken ausfindig machen

„Die Feststellung eines IT-bezogenen Risikos ist lediglich eine Frage eines robusten Risikomanagements", so Wissink und Schütte. ICT-Unternehmen müssen genau feststellen, welche Produkte und Dienstleistungen von ihnen geliefert bzw. erbracht werden, um potenzielle Risiken ausfindig zu machen. Entwickeln sie Software? Vertreiben sie Software? Sind sie ein MSP? Bewahren sie Passwörter für Kunden auf?



x5

„Anstatt eines Hauptrisikos gibt es nun fünf grosse Gefahren. Das Risiko für ICT-Unternehmen ist somit fünf Mal höher als noch vor 10 bis 15 Jahren.“



Ein Information Security Management System (ISMS) ermöglicht es Unternehmen, dies ausfindig zu machen. Diese zentralisierten Rahmenwerke schaffen die Möglichkeit, eigene Informationssicherheitspraktiken zu verwalten, zu überwachen und zu überprüfen.

Die Softwareentwickler widmen der Schaffung eines sicheren Produkts viel Zeit und Mühe. Wissink fügt aber an, dass es in den Umgebungen von Softwareentwicklern jedoch häufig an ähnlichen Schutzvorkehrungen fehlt. Beispielsweise werden Kunden häufig aufgefordert, eine Software von einer nicht gut geschützten Website herunterzuladen.

Stärkung der Verteidigungslinien

Wenn man Cyberangriffe stoppen möchte, bedarf es mindestens standardmässigen Hygienemassnahmen, darunter eine Multi-Faktor-Authentifizierung, angemessene Bewusstseinsschulungen für Mitarbeiter, Firewalls, Scan von Phishing-E-Mails und Filtern von Websites.

„ICT-Unternehmen sollten die absolut bewährtesten Praktiken einführen, wenn man die umfassenderen potenziellen Auswirkungen von Verlusten aus einem breit gefächerten Vorfall und die Sorgfaltspflichten bedenkt“, empfiehlt Wissink. Seiner Ansicht nach benötigen Unternehmen ein Privileged Access Management (PAM) System. Das PAM-Tool schützt die Identität, da es einen speziellen Zugriff oder spezielle Fähigkeiten gewährt, der/die über jene/n von regulären Nutzern hinausgeht. Dies ist besonders für MSPs wichtig, bei denen zahlreiche Personen über ein zentrales Softwarepaket auf mehrere Programme zugreifen.

„Softwareentwickler müssen zudem ihr Netzwerk isolieren und es mit zusätzlichen Tools schützen, auf die nur die Entwickler Zugriff haben“, warnt Wissink. „Die Entwicklungsumgebung sollte keine automatische Verbindung zum Rest des Unternehmens haben.“

Weitere gute Organisationsmassnahmen zur Verringerung der Gefahren und für eine bessere Geschäftskontinuität sind das kontinuierliche Testen von Backups und ihre Offline-Aufbewahrung sowie ein besonders starker Fokus auf der Verschlüsselung von Passwörtern und sonstigen Daten. Die Einstellung eines IT Security Officers ist ebenfalls eine gute Idee.

„Die Unternehmen müssen Passwörter und sonstige Daten schützen. Sie sollten bezüglich der Aufbewahrung und Verarbeitung der Daten ebenfalls über eine gute vertragliche Vereinbarung verfügen“, so Schütte.

Bei der Vorsorge geht es allerdings nicht nur um technische Präventionsmassnahmen. Es geht um Kommunikation anhand vertraglichen Service Level Agreements und Datenschutzvereinbarungen. „Ein ICT-Unternehmen, und insbesondere ein MSP, unterliegt der Sorgfaltspflicht, die eigenen Kunden bezüglich potenzieller schlechter Schutzniveaus einer bestimmten Kundenumgebung zu warnen und entsprechend zu informieren“, fügt Wissink hinzu. „Die Kunden sollten dabei schriftlich informiert werden. Zum Schutz vor Haftungsansprüchen sollte dies zudem dokumentiert werden.“

Schütte zufolge sind ICT-Unternehmen bei der Entwicklung sicherer Entwicklungsrichtlinien im Rückstand. Hierzu zählen Penetrations- und Anfälligkeitstests sowie Codeprüfungen und Schulungen zum Schreiben von Code (OWASP Top Ten kann helfen).

Softwareentwickler, die nicht-kritische Software entwickeln, sollten den Bedarf an diesen Richtlinien nicht ausser Acht lassen.

„Im heutigen Umfeld ist jedes Unternehmen ein potenzielles Angriffsziel“, warnt Wissink.

Das Wichtigste in Kürze

- **Angriffe auf MSPs sind die grösste neue Gefahr** bei der Schadensregulierung
- **ICT-Unternehmen müssen Zero-Day-Angriffe** besser handhaben
- **Die Sorgfaltspflichtrisiken steigen an und** sollten von den Unternehmen berücksichtigt werden
- **Ein Information Security Management System** (ISMS) kann dabei helfen, Risiken zu erfassen
- **Verwenden Sie ein PAM (Privileged Access Management)**-Tool, um Hackern Einhalt zu gebieten
- **Isolieren Sie Ihre Entwicklungsumgebung** vom Rest des Unternehmens
- **Die Kommunikation mit den Kunden ist** ebenfalls wichtig für die Cyberprävention
- **Führen Sie angemessene sichere** Entwicklungsrichtlinien ein
- **Ein Netzwerküberwachungssystem (24/7 überwacht)** ist eine gute Idee
- **Lassen Sie die formellen Krisenbewältigungs-** und Notfallpläne nicht ausser Acht
- **Denken Sie daran, kontinuierlich Backups zu** testen und diese offline aufzubewahren

Erfassung von Verletzungen der Cybersicherheit

Überwachungs- und Erkennungssoftware wie EDR (Endpoint Detection and Response) sind für ICT-Unternehmen ein Muss. Dies ist auch der Fall für Firewalls oder ein Netzwerküberwachungssystem, die 24/7 von einem internen oder externen Security Operations Center überwacht werden. „Sobald ein Hacker es in ein System geschafft hat, muss dies rechtzeitig erkannt werden“, hebt Wissink hervor.

Das Feuer löschen

Sowohl Wissink als auch Schütte sind der Meinung, dass eines der kritischsten Elemente für Unternehmen bei der Handhabung von Cyberangriffen ein klarer Krisenbewältigungsplan ist. Durch eine frühzeitige Notfallplanung kann ein Unternehmen angemessen und schnell auf einen Hackerangriff reagieren. Bei einem Softwareunternehmen geht dieser Plan über seine eigene IT-Umgebung hinaus und sollte ebenfalls eine Richtlinie zur Kundenkommunikation und zum Krisenmanagement beinhalten. Laut ihrer Erfahrung sind zahlreiche Unternehmen nicht vorbereitet. „Zumeist wissen sie nicht, was sie im Krisenfall tun sollen“, so Schütte.

Wenn die Sicherheit der IT-Systeme verletzt wird, müssen die Unternehmen die Sicherheit der Dienste und eine schnellstmögliche Wiederherstellung gewährleisten. Ferner müssen sie auch zeigen, dass sie ihre Kunden in der Zwischenzeit kompetent bedienen können.

Die Zukunft der cyberbezogenen Risiken in der digitalen Ära kann beunruhigend erscheinen. Wenn Sie jedoch nicht die vorbeugenden Schritte zum Schutz Ihres Geschäfts einleiten, ist dies so, als würden Sie die Eingangstüre weit offen lassen und hoffen, dass nichts gestohlen wird. Rein geschäftlich macht es weitaus Sinn, mehr über eine gute IT-Hygiene zu lernen und die richtigen Massnahmen umzusetzen, um sich selbst und die Kunden richtig zu schützen.

Ansprechpartner

Barry Schütte
Manager Industry Practices Benelux, Chubb
bschutte@chubb.com

Wouter Wissink
Senior Principal Cyber Risk Engineer und Technology Industry Practitioner, Chubb
wwissink@chubb.com

Chubb. Insured.℠