Cybersicherheit: Finanzbranche im Fokus

Aktuelle Kaspersky-Studie legt Status Quo der IT-Sicherheit im deutschen Finanzwesen offen

kaspersky BRING ON THE FUTURE

kaspersky.de

Ob Online-Banking, Mobile Payment, Cloud-Lösungen oder künstliche Intelligenz – die Digitalisierung schreitet auch im Finanzwesen weiter voran. Allerdings vergrößern komplexe, digitale Finanztechnologien auch die Angriffsfläche für IT-Sicherheitsbedrohungen, der hohe Grad an Vernetzung macht das Finanzsystem besonders anfällig. Im Zuge der Pandemie hat sich diese Entwicklung weiter beschleunigt, denn Menschen und Unternehmen haben ihre Aktivitäten vermehrt in den virtuellen Raum verlagert. Gleichzeitig ist die Finanzbranche für das öffentliche Leben in Deutschland von hoher Bedeutung. Dies zeigt sich unter anderem daran, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) zahlreiche Unternehmen und Institutionen aus dem Finanzsektor als Betreiber Kritischer Infrastrukturen definiert hat – ähnlich der Energie- oder Trinkwasserversorgung. Entsprechend wichtig ist für deutsche Finanzunternehmen eine nachhaltige und adäquate Cybersicherheitsstrategie und -struktur.

Wie ist es aktuell um die IT-Sicherheit in der deutschen Finanzbranche bestellt? Was sind die größten Bedrohungen? Wie werden Budgets verteilt? Vor welchen Herausforderungen stehen IT-Entscheidungsträger heute, und welche Maßnahmen sorgen für nachhaltigen und wirksamen Schutz vor gegenwärtigen und zukünftigen Cyberbedrohungen?

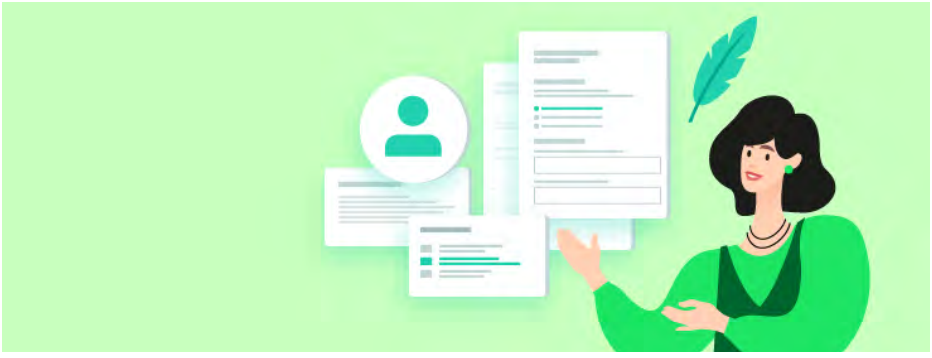
Eine aktuelle Kaspersky-Umfrage zur Cybersicherheitslage der deutschen Finanzbranche gibt Antworten auf diese Fragen. Die Ergebnisse bieten einen Überblick der wichtigsten Bedrohungen derzeit aus Sicht der Betroffenen und zeigen, wie IT-Sicherheitsverantwortliche der Branche die aktuelle Situation einschätzen. Zudem wird deutlich, wie sich Unternehmen und Institutionen wirksam vor einer stetig wachsenden Zahl von Cyberbedrohungen schützen können.

Inhaltsverzeichnis

Methodologie
Die Umfrage wurde von Arlington Research im Auftrag von Kaspersky im Januar 2022 durchgeführt.
Dabei wurden 150 IT-Entscheidungsträger aus der Finanzbranche in Deutschland befragt, davon 78,6 Prozent im höheren und mittleren Management tätig. 54 Prozent der Befragten sind in Unternehmen und Organisationen mit einer Größe von 50 bis 999 Mitarbeitern und 46 Prozent mit mehr als 1.000 Mitarbeitern beschäftigt.

Top-5-Ergebnisse für Deutschland

1. **Vielschichtige Angriffe, hohes Risiko – am häufigsten Angriffe durch Spear Phishing und Ransomware:** Neun von zehn (90,7 Prozent) der befragten Finanzorganisationen waren seit Beginn der Pandemie von mindestens einem Cybersicherheitsvorfall betroffen. Am häufigsten waren Angriffe durch Spear Phishing
2. (40 Prozent) und Ransomware (31,3 Prozent). Auch künftig schätzen knapp drei Viertel der Befragten (71,3 Prozent) die IT-Gefahrenlage für ihr Unternehmen als „hoch" ein. Vor allem IT-Sicherheitsbeauftragte sind dahingehend eher pessimistisch (88,2 Prozent) eingestellt.
3. **Gefühl, guten Schutz gegen Cyberbedrohungen zu haben; gleichzeitig wird Cyberangriffsrisiko als hoch eingeschätzt.** Trotz der Vielzahl an Bedrohungen sehen sieben von zehn Befragten (69,3 Prozent) der Finanzbranche ihr Unternehmen ausreichend gegen Cyberangriffe gerüstet. Auf Geschäftsführerebene sind es sogar drei Viertel (75,4 Prozent). Das stärkste Sicherheitsgefühl (80 Prozent) herrscht in großen Finanzinstituten von 1.000 bis 4.999 Mitarbeitern vor, obwohl hier gleichzeitig das Risiko von Cyberattacken besonders hoch eingeschätzt wird. Insgesamt verweisen drei von vier Befragten (76,7 Prozent) auf Notfallpläne wie einen Business Continuity Plan oder Desaster Recovery Plan in ihrem Unternehmen. Am häufigsten setzen große Finanzinstitute diese Notfallmechanismen ein (87,3 Prozent).
4. **Mitarbeiter als Sicherheitsrisiko:** Der „Faktor Mensch" stellt bei Cyberbedrohungen in der Finanzbranche einen bedeutenden Knackpunkt dar. 38,7 Prozent aller Befragten geben an, dass IT-Sicherheitsvorfälle während der Pandemie auf Mitarbeiter zurückzuführen waren. Die Befragten erkennen hier besondere Herausforderungen bezüglich der IT-Sicherheitsexpertise und des Datenschutzes: als größte Schwachstellen werden Remote-Arbeit (24 Prozent) und das Ignorieren von Unternehmensrichtlinien (18,7 Prozent) genannt. Andererseits mangelt es vielen Mitarbeitern noch immer an einem grundsätzlichen Bewusstsein für Cybersicherheit. Obwohl Finanzunternehmen ihre IT-Mitarbeiter besser als jede andere Branche im Hinblick auf Cybersicherheit schulen, besteht für regelmäßige Schulungen in anderen Abteilungen durchaus Verbesserungspotential.
5. **Das Budget-Paradox: Hohes Sicherheitsrisiko und trotzdem ausreichendes IT-Sicherheitsbudget?** Sieben von zehn IT-Entscheidungsträgern in Finanzunternehmen (71,3 Prozent) schätzen die Cyberbedrohungslage als hoch ein. Dennoch finden zwei Drittel der Befragten (67,3 Prozent), dass ihr IT-Sicherheitsbudget für die kommenden zwei Jahre ausreichend ist und über die Hälfte (54,7 Prozent) glaubt, dass sie intern nicht über das nötige Know-How verfügt, um sich umfassend gegen Cyberbedrohungen zu schützen. Deshalb setzen 52,7 Prozent auf externe Dienstleister – vor allem kleinere Unternehmen mit einer Mitarbeiteranzahl von 50 bis 249 (67,9 Prozent) tun dies.
6. **Threat Intelligence: Kommt zum Einsatz, aber noch nicht überall wo gewünscht:** Insgesamt nutzen laut den Studienergebnissen stolze 98,7 Prozent der Finanzinstitute mindestens einen Threat-Intelligence-Security-Service, um sich vor der immer komplexer werdenden Bedrohungslandschaft zu schützen. Am beliebtesten sind Services zur Malware-Analyse (65,3 Prozent) sowie APT-Reporting (56,7 Prozent) und Threat Data Feeds (54,7 Prozent). Allerdings nutzen noch nicht alle Unternehmen die Services, die sie gerne einsetzen würden. Beim Thema Sicherheitsbewertungen, zum Beispiel über das TIBER Framework, plädieren 34,4 Prozent dafür, dass derartige Services in ihrem Unternehmen genutzt werden sollten. Knapp ein Drittel (32 Prozent) wünscht sich den Einsatz von Threat Data Feeds in ihrer Organisation.



„Egal ob Ransomware, Phishing, zielgerichteter Angriff oder ‚nur' generische Malware, die Finanzbranche sieht sich mit einer vielfältigen Bedrohungslandschaft konfrontiert. Es ist daher nicht verwunderlich, dass die von uns befragten IT-Entscheider die Gefahrenlage in Deutschland als hoch einschätzen. Finanzinstitute sehen sich zwar ausreichend gegen Cyberangriffe gerüstet, weil sie unter anderem Notfallpläne zur Hand haben. Die Branche muss dennoch mehr in IT-Sicherheit investieren. Denn ein erfolgreicher Angriff kann zu Verlust von Daten, Geld und Kunden führen. Wir empfehlen einen umfassenden, mehrstufigen Cybersicherheitsansatz, der alle möglichen Einfallstore abdeckt."

Waldemar Bergstreiser,
Head of Channel Germany
bei Kaspersky.

Status Quo der Cybersicherheitslage im Finanzwesen

71,3 Prozent der befragten IT-Entscheidungsträger im deutschen Finanzsektor stufen die aktuelle Bedrohungssituation für die Cybersicherheit in ihrem Unternehmen als „hoch" ein. Besonders IT-Sicherheitsbeauftragte sind pessimistisch (88,2 Prozent), aber auch die Bedrohung für Unternehmen mit 1.000 bis 4.999 Mitarbeitern wird überdurchschnittlich hoch (81,8 Prozent) eingeschätzt.

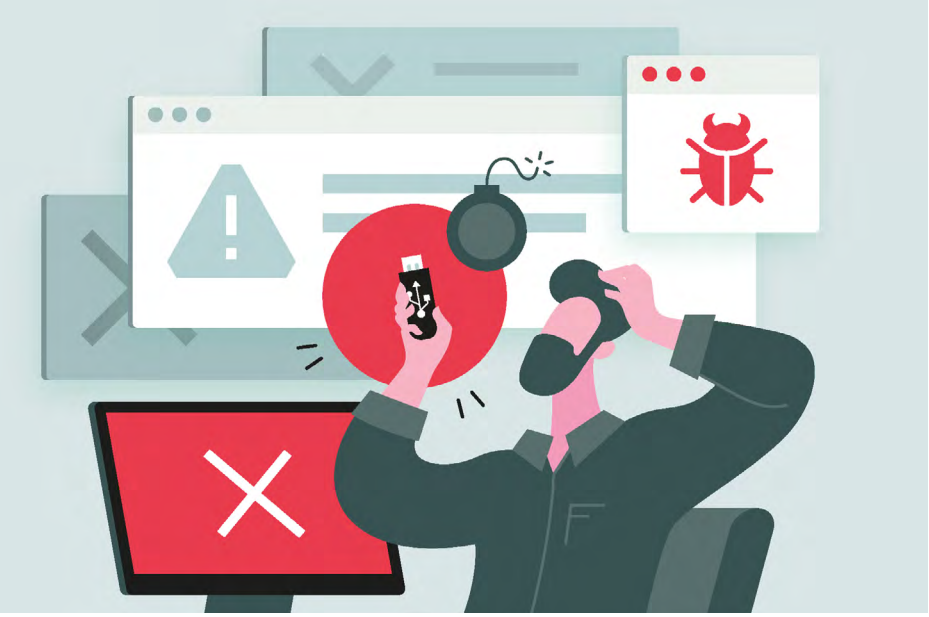
Insgesamt berichten die befragten Entscheider von vielfältigen Bedrohungen seit Beginn der Pandemie. Neun von zehn Befragten (90,7 Prozent) geben an, dass ihr Unternehmen in diesem Zeitraum von Sicherheitsvorfällen betroffen war. Die Arten der Angriffe waren so unterschiedlich wie vielschichtig: Vier von zehn befragten Entscheidern berichten von Spear Phishing (40 Prozent), fast ein Drittel war von Ransomware-Angriffen (31,3 Prozent) und von DDoS-Attacken (30,7 Prozent) betroffen. Gut ein Viertel der Befragten hatte mit Spyware (27,3 Prozent) und generischer Malware (26 Prozent) zu kämpfen; 16,7 Prozent haben zielgerichtete Attacken erlebt. Eine Führungskraft (C-Suite) eines mittelgroßen Unternehmens (500 bis 999 Mitarbeiter) verweist auch in der qualitativen Befragung auf die Gefahren: **„Die meisten Cybersicherheitsprobleme entstehen durch Spear-Phishing-Attacken und das ist sehr ernst zu nehmen."** Ein IT-Sicherheitsspezialist eines kleinen Unternehmens (50 bis 249 Mitarbeiter) fürchtet **„DDoS-Angriffe, weil diese unsere digitalen Services einschränken oder lahmlegen würden".**

Trotz der vielfältigen Bedrohungen sehen sieben von zehn Befragten (69,3 Prozent) in der Finanzbranche ihr Unternehmen ausreichend gegen Cyberangriffe gerüstet. Auf Geschäftsführerebene sind es sogar drei Viertel (75,4 Prozent). Drei von vier Befragten (76,7 Prozent) verweisen auf vorhandene Notfallpläne in ihrem Unternehmen, wie einen Business Continuity oder Desaster Recovery Plan, der regelmäßig getestet wird. Insgesamt herrscht das stärkste Sicherheitsgefühl in großen Finanzinstituten von 1.000 bis 4.999 Mitarbeitern, obwohl hier gleichzeitig das Risiko besonders hoch eingeschätzt wird. Vier von fünf Befragten (80 Prozent) sind der Meinung, dass Unternehmen dieser Größe gut gegen IT-Sicherheitsbedrohungen geschützt seien. Mit 87,3 Prozent setzen diese auch am häufigsten Desaster Recovery Pläne ein.

76,7 Prozent der Befragten aus der Finanzbranche möchten gerne mit einem externen Sicherheitspartner zusammenarbeiten. Unter großen Unternehmen mit mehr als 1.000 Mitarbeitern ist die Zustimmung sogar noch deutlich größer (88,4 Prozent).

Stimmen aus der Branche: Welche Cybersicherheitsaspekte halten die Finanzbranche nachts wach?

Im Rahmen der Studie konnten sich die Teilnehmer auch offen, in einem freien Text, über ihre Einschätzung der Cybersicherheit in ihren Unternehmen und die damit zusammenhängenden Herausforderungen äußern. Es wird deutlich, dass ein grundsätzliches Bewusstsein für IT-Sicherheitsgefahren in der Finanzbranche vorhanden ist .



Aussagen von Führungskräften

„Man kann kaum auf alle Attacken vorbereitet sein“, erklärt ein Senior Manager (C-Suite) einer kleineren Firma mit 50 bis 249 Mitarbeitern. Dieser Aussage stimmt auch die Führungskraft (C-Suite) eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter) zu: **„Die Bedrohung durch externe Angriffe auf unser System ist sehr groß – sehr viel Cyberspace-Crime zur Zeit.“** Ein IT-Mitarbeiter aus dem mittleren Management eines großen Unternehmens beklagt die **„Zunahme immer komplexerer Cyberangriffe, teils mit Unterstützung von Staaten“**. Spezifischer wird ein Mitglied der C-Suite eines weiteren großen Unternehmens: Er sorgt sich vor **„Attacken, die dazu führen, dass das Unternehmen die IT-Services für seine Kunden über einen längeren Zeitraum nicht ausüben kann, was zu Kursverlusten und Schadensfällen führen würde.“** Ein IT-Spezialist eines großen Unternehmens fürchtet ebenfalls **„Kursverluste, weil keine Aufträge an die Börsen geroutet werden können“**. Insgesamt macht sich die Management-Ebene vor allem Sorgen um die negativen Folgen eines IT-Sicherheitsvorfalls für das Unternehmen und den Imageverlust, wenn es zu finanziellen Schäden oder zum Verlust sensibler Daten kommen sollte.

Aussagen der IT-Experten

Auf der IT-Ebene kreisen die Gedanken der Befragten hingegen größtenteils um die internen Problembereiche, die einen Cyberangriff zulassen könnten – oder aber um den Mangel an präventiven Maßnahmen, um einen Sicherheitsvorfall zu verhindern. Ein IT-Spezialist eines großen Unternehmens beklagt, **„dass die Unachtsamkeit mancher MitarbeiterInnen ein großes Einfallstor für Cyberattacken bleibt“**. Ein weiterer Experte einer großen Organisation fürchtet **„Mitarbeiter, die gezielt Maßnahmen untergraben“**. Ein IT-Sicherheitsexperte – ebenfalls bei einem großen Unternehmen tätig – befürchtet **„mehr Angriffsfläche aufgrund vermehrter Remote-Arbeitsplätze im Home Office“**. Die größte Sorge eines IT-Mitarbeiters aus dem mittleren Management besteht darin, **„dass Sicherheitslücken von Hackern ausgenutzt werden“**. Der IT-Spezialist eines mittelgroßen Unternehmens (250 bis 499 Mitarbeiter) befürchtet, **„dass unsere IT-Kräfte zu wenige Kenntnisse haben“**. Ein weiterer IT-Spezialist eines großen Unternehmens formuliert es folgendermaßen: **„Die größte Bedrohung in der IT sind unbemerkte Angriffe mit erheblichen finanziellen Schäden.“**

„Der Fachkräftebedarf in Deutschland nimmt – wie auch in anderen europäischen Ländern – in allen Branchen zu; allein im Security-Bereich werden mehrere Tausend Experten benötigt. Davon sind kleine wie auch große Unternehmen gleichermaßen betroffen. Wir sehen die Tendenz, dass Unternehmen mit fehlenden Ressourcen ihre Cybersicherheitsabteilung an einen Dienstleister outsourcen, um trotz Fachkräftemangel umfassend geschützt zu sein – und das ist eine gute Entscheidung! Denn Unternehmen in Europa, die auf externe Experten setzen, sind besser geschützt: sie werden mit fast 10 Prozent weniger Cybervorfällen konfrontiert als Unternehmen, die vollständig oder überwiegend mit internen Ressourcen arbeiten."

Waldemar Bergstreiser,
Head of Channel Germany
bei Kaspersky.

Herausforderungen, Risiken und Konsequenzen

Herausforderungen für die Cybersicherheit in der Finanzbranche

Einerseits fühlen sich sieben von zehn Befragten in der Finanzindustrie gut gegen mögliche Cyberangriffe gerüstet. Gleichzeitig geben aber mehr als die Hälfte (54,7 Prozent) der Umfrageteilnehmer an, dass sie nicht über die interne IT-Sicherheitsexpertise verfügen, um vollständig vor Bedrohungen geschützt zu sein. Dabei ist die Zustimmung in der IT (64,4 Prozent) deutlich größer als bei den Führungskräften (45,6 Prozent). Ein IT-Mitarbeiter eines Großunternehmens mit mehr als 5.000 Mitarbeitern bringt es im Rahmen der Kaspersky-Studie auf den Punkt: **„Es ist schwierig, mit der Bedrohungslage Schritt zu halten. Das Feld ist so groß, dass eine hohe Zahl an Experten benötigt wird, die im Markt schwer rekrutierbar ist."** Ein weiterer IT-Sicherheitsexperte eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter) stimmt zu: **„Wir haben ein Personalproblem, das sich negativ auf unsere Bedrohungsabwehr auswirkt."**

Eine weitere große Herausforderung sehen die Befragten in den ständig wachsenden Vorgaben: So geben 59,3 Prozent an, dass die zunehmende Belastung durch Vorschriften und Regularien das Risiko erhöhe, dass diese nicht eingehalten werden. Ganz besonders gilt das in kleineren Unternehmen von 250 bis 499 Mitarbeitern (71,4 Prozent).
Ein IT-Sicherheitsexperte eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter) formuliert es so: **„Unsere größte Sorge ist die Uneinsichtigkeit der Mitarbeiter Sicherheitsregeln einzuhalten."**

Risiken für die Cybersicherheit in der Finanzbranche

Mitarbeiter als Einfallstor für Cyberangriffe

Sind die Mitarbeiter also tatsächlich ein nicht zu vernachlässigendes Einfallstor in Unternehmensnetzwerke? Die Erkenntnisse der aktuellen Studie von Kaspersky deuten darauf hin. Sowohl die Untersuchungsergebnisse als auch die Aussagen der befragten Entscheider lassen den Schluss zu, dass der „Faktor Mensch" bei Cyberbedrohungen in der Finanzbranche einen bedeutenden Knackpunkt darstellt. So geben 38,7 Prozent aller Befragten an, dass IT-Sicherheitsvorfälle während der Pandemie auf Mitarbeiter zurückzuführen waren. Besondere Herausforderungen sehen die Befragten bezüglich der IT-Sicherheitsexpertise und des Datenschutzes: Hier werden das Ignorieren von Unternehmensrichtlinien (18,7 Prozent), Remote Arbeit (24 Prozent) und Schatten-IT (11,3 Prozent) als größte Schwachstellen genannt. **„Schatten-IT ist gerade unsere größte Sorge, da eine Menge Mitarbeiter wegen der Pandemie im Home Office arbeitet und dort viel lässiger ist und Richtlinien missachtet"**, erklärt eine Führungskraft eines kleineren Unternehmens (250 bis 499 Mitarbeiter). Viele Umfrageteilnehmer stoßen mit ihren Aussagen ins gleiche Horn: **„Die eigenen internen Mitarbeiter sind nach wie vor die größte Gefahrenquelle"**, sagt ein Befragter aus dem mittleren Management einer großen Firma. **„Die größte Sorge in Bezug auf die IT-Sicherheit in unserem Unternehmen ist das unbefugte Benutzen von fremden Geräten durch Mitarbeiter"**, meint eine Führungskraft eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter). In weiteren Statements über alle Unternehmensgrößen hinweg ist die Rede von **„Mitarbeitern, die gezielt Maßnahmen untergraben"**, **„Unachtsamkeit von Mitarbeitern"** oder auch **„Schäden, die bewusst durch Mitarbeiter verursacht werden"**.

„Unsere Studie zeigt: Die Finanzbranche sieht die eigenen Mitarbeiter als das größte Sicherheitsrisiko für ihre Organisation. Es gilt, die eigene Belegschaft mit ins Cybersicherheitsboot zu holen. Aufklärung und Schulungen sind neben dem Einsatz starker technologischer Lösungen das A und O. Ein zeitgemäßes Schulungsprogramm kann von Abteilung zu Abteilung individuell erstellt werden und muss in den Arbeitsalltag integriert werden. Mitarbeiter müssen die möglichen Angriffsvektoren der Cyberkriminellen, wie auch die Konsequenzen ihres eigenen Handelns verstehen. Denn ein falscher Klick auf einen schädlichen Anhang oder Link öffnet Cyberkriminellen Tür und Tor ins Unternehmensnetzwerk. Schulungen müssen das komplette Personal adressieren – vom Empfang bis zur Führungsriege."

Waldemar Bergstreiser,
Head of Channel Germany
bei Kaspersky.

Auch die Zahlen der Studie belegen, dass es vielen Mitarbeitern im Finanzsektor am Bewusstsein für Cybersicherheit mangelt – und dass beim Schulungspotenzial durchaus noch Luft nach oben besteht. Zwar werden in mehr als der Hälfte der Organisationen (50,7 Prozent) alle IT-Mitarbeiter regelmäßig zu Sicherheitsthemen und -verfahren geschult, in den restlichen Abteilungen, wie zum Beispiel Assistenten der Geschäftsleitung, Marketing, Analysten und Händler, Buchhaltung, ist die Situation allerdings weniger beruhigend: Zwischen 25,3 und 32 Prozent der Befragten geben an, dass in allen anderen Abteilungen weniger als die Hälfte der Mitarbeiter regelmäßig geschult werden. Ein IT-Mitarbeiter bei einem großen Unternehmen (1.000 bis 4.999 Mitarbeiter) formuliert es kurz und prägnant: **„Die Anwender bei uns sind sehr unwissend."**

Ebenfalls spannend: Weitere „übliche Verdächtige" der IT-Sicherheitsrisiken spielen in der Finanzbranche nur eine untergeordnete Rolle. So geben nur 6,7 Prozent der Befragten an, dass seit Beginn der Pandemie ungepatchte Programme als Türöffner zum Netzwerk ihres Unternehmens dienten. Noch weniger (6 Prozent) berichten von Angriffen, die über einen externen Dienstleister oder eine Partnerorganisation geführt wurden.

Das Budget-Paradox

Einerseits schätzen fast drei Viertel (71,3 Prozent) der befragten Entscheidungsträger in Finanzinstituten die IT-Bedrohungslage als „hoch" ein. Dennoch sind gleichzeitig mehr als zwei Drittel (67,3 Prozent) dieser so antwortenden Untersuchungsteilnehmer der Meinung, dass ihr IT-Sicherheitsbudget für die kommenden zwei Jahre ausreichend sei. Befragte aus kleinen Unternehmen (50 bis 249 Mitarbeiter) zeigen hier die größte Zuversicht (78,6 Prozent). Mit Blick auf die Budgetfrage „unentschieden" zeigen sich knapp ein Viertel der Befragten (24 Prozent). Im Senior Management sind hingegen knapp drei Viertel der Befragten (73,2 Prozent) davon überzeugt, dass das IT-Sicherheitsbudget für die kommenden zwei Jahre genüge. Bei der qualitativen Befragung im Rahmen der Studie gab es allerdings abweichende Meinungen: Ein IT-Sicherheitsmitarbeiter eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter) gab zu Protokoll: **„Ich glaube nicht, dass unser Budget für das Ausmaß der Bedrohungen, denen wir ausgesetzt sind, angemessen ist."**

Etwa sieben von zehn Entscheidern (69,3 Prozent) geben an, dass die derzeitigen Maßnahmen ausreichten, um die eigene Organisation vor Cyberangriffen zu schützen. Die Zustimmung von Führungskräften aus der C-Suite (75,4 Prozent) ist dabei deutlich höher als die der IT-Mitarbeiter (59,3 Prozent). Befragte aus großen Unternehmen (1.000 bis 4.999 Mitarbeiter) halten ihre IT-Sicherheitsmaßnahmen sogar zu 80 Prozent für genügend. Interessanterweise geben fast drei Viertel (73,6 Prozent) der Befragten an, dass die Anstrengungen ihres Unternehmens zur Cybersicherheit ausreichend seien, obwohl sie ausdrücklich eine schwerwiegende Gefahrenlage wahrnehmen. Knapp über die Hälfte der Befragten (52,7 Prozent) gibt zu Protokoll, dass ihr Unternehmen auf den Support externer Cybersicherheitsexperten zurückgreife. Besonders kleinere Unternehmen (50 bis 249 Mitarbeiter) nehmen diesen Service in Anspruch (67,9 Prozent).

„Der Mehrwert von Cybersicherheit wird von den IT-Entscheidern innerhalb der Finanzbranche unterschätzt. Dass zwei Drittel der Befragten ihr Budget für Cybersicherheit in den kommenden Jahren als ausreichend erachten, ist eindeutig zu wenig – zwischen 90 und 100 Prozent sollten es sein. Auch wenn sich viele als gut geschützt sehen, sollte insbesondere die Finanzbranche in puncto Cyberabwehr, Datensicherung und Spionage nicht sparen – denn jeder Euro, der in den kommenden Jahren in die Cybersicherheit gesteckt wird, wird sich auszahlen und ist im Endeffekt mittel- und langfristig gut angelegtes Geld."

Waldemar Bergstreiser,
Head of Channel Germany
bei Kaspersky.

Konsequenzen: Wovor sich die Finanzbranche fürchtet

Im Rahmen der Kaspersky-Studie wurden die Entscheider in Finanzinstitutionen auch danach gefragt, welche Konsequenzen eines möglichen Cyberangriffs sie am meisten fürchten. Die Antworten fielen vielschichtig aus: Knapp die Hälfte der Befragten (48,7 Prozent) fürchtet den Diebstahl und Verkauf sensibler Kundendaten. 44 Prozent sorgen sich um einen Imageverlust des Unternehmens durch die unzureichende Einhaltung der Informationssicherheit, 42,7 Prozent befürchten finanzielle Verluste für die Organisation und ihre Kunden. Ungefähr genauso viele glauben, dass ein Sicherheitsvorfall sie viele Kunden kosten könnte (42 Prozent).

Ein ähnliches Bild ergibt sich, wenn man sich die Aussagen aus der qualitativen Befragung ansieht. Ein IT-Mitarbeiter eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter) sorgt sich, **„dass sensible Kundendaten aufgegriffen werden. Die Auswirkungen wären fatal für unser Unternehmen."** Immer wieder wird – über alle Unternehmensgrößen hinweg – der Verlust sensibler Daten erwähnt. Ein Mitglied der Geschäftsführung (C-Suite) eines großen Unternehmens (1.000 bis 4.999 Mitarbeiter) sagt, seine größte Sorge sei **„das Hacken von Kundendaten. Damit wäre ein immenser Vertrauens- und Imageschaden verbunden."** Ein IT-Mitarbeiter aus derselben Unternehmensgröße hat Bedenken, dass „falsche oder gehackte Geldtransaktionen ins Ausland, an Betrüger oder Terrorstaaten" gehen. Ein Senior Manager eines mittelgroßen Unternehmens befürchtet **„einen Angriff, der unserem Unternehmen schadet, der Entwicklung schadet und dazu führt, dass Investoren verloren gehen."**

Maßnahmen gegen Cyberbedrohungen in der Finanzbranche: Kombination aus Mensch und Technologie ist der Schlüssel

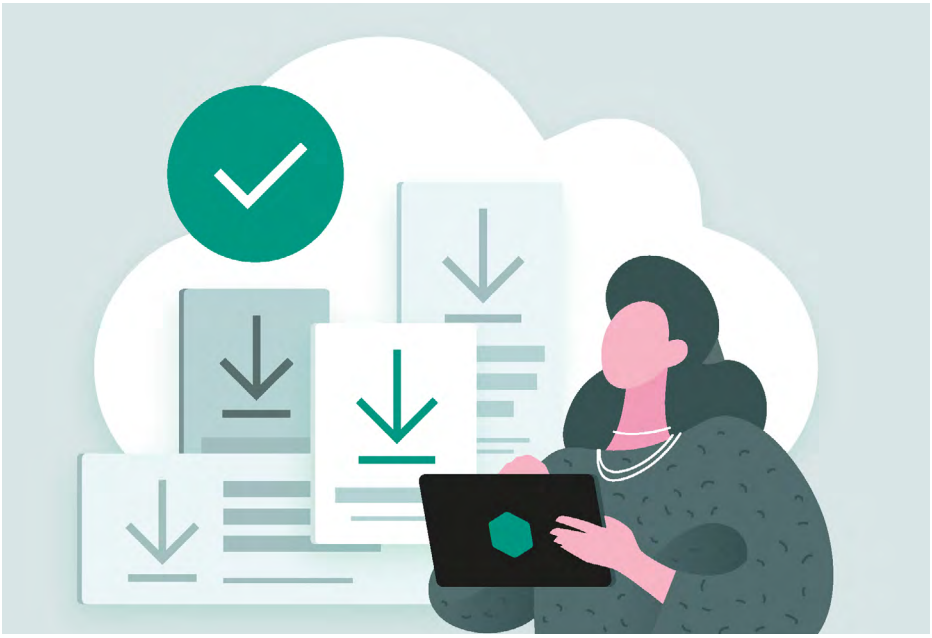
Die Finanzbranche in Deutschland ist mit Blick auf Cyberbedrohungen besonders gefährdet. Dies liegt zum einen am Grad der Digitalisierung im Finanzwesen, der seit Beginn der Pandemie noch stärker geworden ist. Zum anderen ist die Finanzbranche für Cyberkriminelle attraktiv, weil hier starke Geldflüsse stattfinden und eine riesige Menge an sensiblen Kundendaten von Unternehmen und Institutionen verwaltet wird. In der Studie wird deutlich, dass die Befragten der Finanzbranche sich dieser Sonderrolle durchaus bewusst sind. Der Großteil der Umfrageteilnehmer weiß zudem, dass für umfassende IT-Sicherheit eine Kombination aus technischer Lösung, Threat Intelligence Services und genereller Awareness aller Mitarbeiter notwendig ist.

Technische Lösungen als Basis

Das Fundament eines umfassenden Cybersicherheitskonzepts ist eine technische Lösung zur Abwehr von Angriffen. Immerhin ein Viertel der Befragten (26,7 Prozent) gibt an, dass ihr Unternehmen die derzeitige IT-Sicherheitslösung evaluiert und/oder nach einer neuen Lösung Ausschau hält. Des Weiteren vertrauen alle Befragten bereits heute auf vielschichtige technische Lösungen: Mehr als die Hälfte der Befragten (52,7 Prozent) haben externe IT-Sicherheitsdienstleister, inklusive Threat Intelligence-Services, beauftragt, fast ebenso viele (52 Prozent) nutzen intern präventive Tools und Expertise zur Erkennung und Analyse von Cyberbedrohungen. Jedes zweite Unternehmen (53,3 Prozent) setzt zudem dezidierte Sicherheits-Tools oder -Services ein, um Cloud-Software und -Aktivitäten zu schützen. 37,3 Prozent arbeiten mit Netzwerk-Segmentierung, 36,7 Prozent betreiben ein eigenes Security Operations Center (SOC). Knapp ein Drittel der Befragten (32,7 Prozent) gibt an, dass ihr Unternehmen ein Security Information and Event Management, kurz SIEM, nutzt.

Mitarbeiterschulungen als Ergänzung

Regelmäßige Mitarbeiterschulungen sind eine wichtige Ergänzung zu technologischen Schutzlösungen. Dies scheint – zumindest teilweise – in den Köpfen der Entscheider der Finanzbranche angekommen zu sein: In mehr als der Hälfte der Organisationen (50,7 Prozent) werden 100 Prozent aller Mitglieder der IT-Abteilung regelmäßig zu Sicherheitsthemen und -verfahren geschult. In den restlichen abgefragten Abteilungen (zum Beispiel Assistenten der Geschäftsleitung, Marketing, Analysten und Händler, Buchhaltung) sieht es weniger gut aus. Über ein Viertel der Befragten (zwischen 25,3 Prozent und 32 Prozent je nach Abteilung) geben an, dass hier weniger als die Hälfte der Beschäftigten regelmäßig zu IT-Sicherheitsthemen geschult wird.

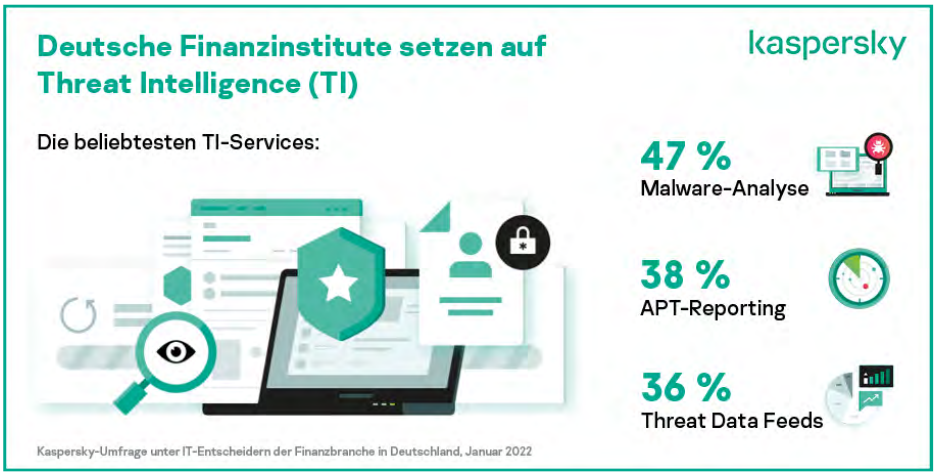


„Gartner definiert Threat Intelligence als einen Schlüsselaspekt innerhalb einer unternehmerischen Sicherheitsarchitektur, der technischen Fachkräften im Bereich Sicherheit und Risikomanagement dabei hilft, Bedrohungen zu erkennen, zu segmentieren und genau zu untersuchen. Heutzutage reicht ein reaktiver Ansatz für die Cybersicherheit einfach nicht mehr aus und eine qualitativ hochwertige Threat Intelligence muss eine Reihe von Merkmalen voraussetzen. Dazu zählen – erstens – ein umfangreicher Kontext, der aus Daten verarbeitbare Intelligenz schafft und einen Mehrwert bietet, und – zweitens – die Unterstützung durch ein anerkanntes Expertenteam mit nachgewiesener Erfahrung in der Aufdeckung komplexer Bedrohungen. Drittens bedarf es einer reibungslosen Integration der Dienste in die bestehenden Sicherheitsabläufe eines Unternehmens. Eine gute Threat Intelligence entlastet interne Cybersecurity-Abteilungen, damit sich diese auf vorrangigere Ziele konzentrieren können."

Waldemar Bergstreiser,
Head of Channel Germany
bei Kaspersky.

Threat Intelligence rundet Sicherheitsansatz ab

Unternehmen im Finanzsektor setzen fast durchgängig auf Threat-Intelligence-Services, wie die Kaspersky-Studie zeigt. Insgesamt nutzen 98,7 Prozent mindestens einen entsprechenden Dienst. Allerdings nutzen noch nicht alle Unternehmen die Services, die sie gerne einsetzen würden. So geben 56,7 Prozent der Untersuchungsteilnehmer an, dass ihr Unternehmen APT-Reports nutzt, um über die neuesten Untersuchungen, Bedrohungskampagnen und Techniken von APT-Akteuren auf dem Laufenden zu sein. Weitere 27,9 Prozent wünschen sich den Einsatz solcher Reports. Gut die Hälfte der Unternehmen (54,7 Prozent) nutzt Threat Data Feeds, weitere 32 Prozent würden dieses Tool in Zukunft gerne nutzen. Malware-Analysen werden von knapp zwei Drittel (65,3 Prozent) der Finanzinstitutionen genutzt, 15,6 Prozent wünschen sich den Einsatz. Rund die Hälfte der Befragten (46,7 Prozent) berichtet, dass ihr Unternehmen Sicherheitsbewertungen beispielsweise über das TIBER-Framework (Threat Intelligence-based Ethical Red Teaming) sowie Tools zur Entdeckung zielgerichteter Attacken (52 Prozent) nutzt. Weitere 34,4 Prozent (Sicherheitsbewertungen) bzw. 25,4 Prozent (Entdeckung zielgerichteter Attacken) der Befragten sind der Meinung, dass ihr Unternehmen entsprechende Tools künftig einsetzen sollte. Insgesamt ist das Bewusstsein für den Einsatz von Threat-Intelligence-Services in der Finanzbranche recht hoch.



IT-Sicherheitslösungen für die Finanzbranche

Kaspersky bietet ein umfangreiches Lösungs-Portfolio für die Finanzbranche, um alle Daten und Assets zu schützen, die ständige Verfügbarkeit der Leistungen sicherzustellen, den Schutz geistigen Eigentums zu gewährleisten und dadurch die Expertise und den Ruf der eigenen Einrichtung zu schützen.

Weitere Informationen unter
https://www.kaspersky.de/enterprise-security/finance

Cyber Threats News: https://securelist.com/
IT-Sicherheitsnachrichten: kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

kaspersky.de

kaspersky BRING ON THE FUTURE