HarfangLab

DIE CYBERRESILIENZ EUROPÄISCHER KMU IN ZEITEN DER MULTIKRISE

Ein Report von HarfangLab zu Cyberrisiken, -strategien und -resilienz in der aktuellen und zukünftigen Bedrohungslandschaft.

2024

HarfangLab

HARFANGLAB REPORT 2024: CYBERBEDROHUNGEN – RISIKEN, RESILIENZ UND STRATEGIEN

ÜBERBLICK

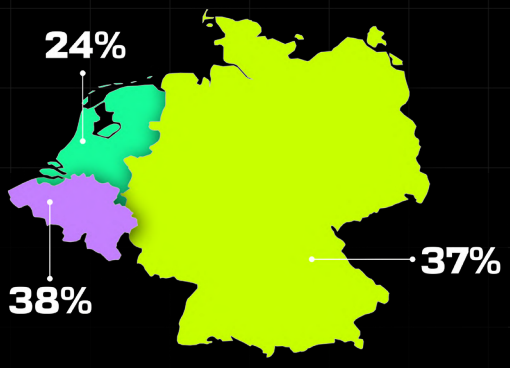
Das Jahr 2024 markiert einen Wendepunkt. Angesichts zunehmender geopolitischer Spannungen sind europäische Organisationen stärker denn je Cyberbedrohungen ausgesetzt. Doch wie gut sind gerade kleine und mittlere Unternehmen (KMU) in Europa auf die kommenden Herausforderungen vorbereitet?

KMU bilden das Rückgrat der europäischen Wirtschaft – die Verbesserung ihrer Cyberresilienz ist daher von entscheidender Bedeutung. Obwohl sie denselben Bedrohungen wie Großunternehmen ausgesetzt sind, verfügen sie über deutlich weniger Ressourcen zur Abwehr.

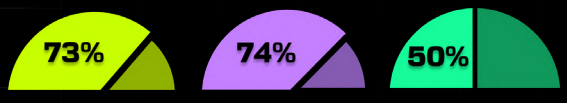
Unsere Untersuchung zielte darauf ab, die Widerstandsfähigkeit kleiner und mittlerer Unternehmen in Europa gegenüber Cyberrisiken zu bewerten. Wie nehmen sie die Bedrohungslage wahr? Welche Schutzmaßnahmen ergreifen sie? Und wie beeinflussen die neuen EU-Compliance-Anforderungen ihre Strategien? Zu diesem Zweck haben wir eine Umfrage unter 750 IT-Entscheidungsträgern aus Frankreich, Deutschland, Belgien und den Niederlanden in Auftrag gegeben.

HIER SIND EINIGE UNSERER WICHTIGSTEN ERGEBNISSE:

Belgische Unternehmen schätzen die Cyberbedrohung am höchsten ein: laut 38 Prozent der belgischen Befragten ist das Bedrohungslevel sehr oder extrem hoch. Ähnlich sehen das 37 Prozent der deutschen und 24 Prozent der niederländischen Unternehmen.

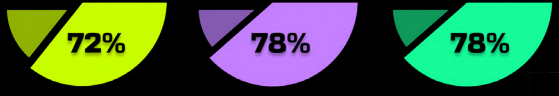


Laut 72 Prozent der Befragten sind europäische Cybersicherheitsdienstleister besser in der Lage, Beratungsleistungen und Produkte anzubieten, die auf die Bedürfnisse der europäischen KMU abgestimmt sind.



IT-Sicherheitsverantwortliche aus Deutschland (73 %) und Belgien (74 %) sind stärker davon überzeugt, dass EU-Regulierungen rund um Cybersicherheit und Datenschutz einen Wettbewerbsvorteil darstellen als ihre niederländischen Kollegen (50 %).

Alle Befragten bevorzugen europäische Cybersicherheitspartner (DE 72 %, BE 78 %, NL 78 %).



IT-Sicherheitsverantwortliche sind davon überzeugt, dass europäische Cybersicherheitspartner besser auf ihre Bedürfnisse eingehen können (DE 72 %, BE 74 %, NL 74 %).

EINLEITUNG:

Organisationen weltweit sind stärker denn je Cyberbedrohungen ausgesetzt. Die aktuelle internationale Lage – einschließlich geopolitischer Konflikte, wirtschaftlicher und politischer Instabilität sowie hoher Inflationsraten – treibt die Kriminalitätsrate in die Höhe und bietet böswilligen Akteuren Anreize für lukrative, aber schädliche Ransomware-Angriffe. Zudem war die Welt noch nie so vernetzt wie heute. In der Post-COVID-Ära hat die Vernetzung innerhalb von Unternehmen zugenommen, was eine größere Angriffsfläche und eine komplexere IT-Landschaft zur Folge hat. Neue Technologien wie generative Künstliche Intelligenz (KI) erfordern zusätzliche Sicherheitsmaßnahmen. Endpunkte dienen dabei als Zugangspunkte zur IT-Infrastruktur eines Unternehmens. Während Unternehmen Technologien zur Endpunkt-Erkennung und -Reaktion (EDR) einsetzen, entwickeln Angreifer ständig neue Taktiken und suchen nach weiteren Zugangsmöglichkeiten, was zu einem ständigen Wettlauf führt.

Europäische Organisationen sind besonders anfällig für Cyberangriffe. Der Kontinent und seine Unternehmen werden als wohlhabend wahrgenommen und sind daher attraktive Ziele. Die zahlreichen Sportereignisse in diesem Jahr – wie die Olympischen Spiele in Paris und die Fußball-Europameisterschaft in Deutschland – haben die Aufmerksamkeit der Weltöffentlichkeit auf sich gezogen und Bedrohungsakteuren neue Angriffsmöglichkeiten geboten. Die europäischen Cyberabwehrsysteme könnten dabei an ihre Grenzen geraten: Berichten[1] zufolge hatten sich die Organisatoren der Olympischen Spiele in Paris auf ein nie dagewesenes Ausmaß an Bedrohungen vorbereitet. Dabei erwarteten sie, dass sich die Zahl der Cybersicherheitsvorfälle im Vergleich zu den Spielen in Tokio im Jahr 2021 verzehnfacht.

Die meisten europäischen Unternehmen sind sich der Bedrohung bewusst. Sie müssen jedoch die Notwendigkeit erhöhter Cybersicherheit gegen knappe Budgets, konkurrierende Prioritäten und die schwierige Rekrutierung und Bindung von Talenten im Bereich Cybersicherheit abwägen. IT- und Sicherheitsverantwortliche stehen vor der Herausforderung, das Bewusstsein im gesamten Unternehmen zu schärfen: Wie können sie allen Mitarbeitenden vermitteln, dass jeder Einzelne einen Beitrag zur Verringerung des Cyberrisikos leisten kann?

In diesem Kontext besteht ein Bedarf an Regulierungen, die Orientierungshilfe in Bezug auf Cybersicherheit bieten. Die Europäische Union ist in dieser Hinsicht weltweit führend. Rechtsvorschriften wie die Datenschutz-Grundverordnung (DSGVO), der Digital Operational Resilience Act (DORA) und die zweite Richtlinie zur Netz- und Informationssicherheit (NIS-2) setzen hohe und einheitliche Standards für Cybersicherheit in allen Mitgliedstaaten. Diese Vorschriften senden ein klares Signal an Unternehmen, Cybersicherheit und Datenschutz höchste Priorität einzuräumen. Doch wie bewerten europäische Unternehmen diese Vorschriften?

1 - Reuters, Paris 2024 bereitet sich auf eine noch nie dagewesene Bedrohung der Cybersicherheit, abgerufen am15. Mai 2024)

Es ist wichtig, dass das regulatorische Umfeld keine zusätzliche Belastung für Unternehmen darstellt. Andernfalls würde die ohnehin schon große Kluft zwischen Chief Information Security Officers (CISOs) und anderen Führungskräften sowie dem Rest der Organisation weiter vergrößert. CISOs werden manchmal als Hindernis für Unternehmen angesehen – was nicht der Fall sein sollte. Wie können sie sicherstellen, dass die Einhaltung von Vorschriften nicht nur als formale Pflicht angesehen wird, sondern tatsächlich zur Sicherheit beiträgt?

In einer sich ständig weiterentwickelnden digitalen Welt ist Cybersicherheit eine Frage der Anpassungsfähigkeit. In Zeiten knapper Budgets und notwendiger Prioritätensetzung stellt sich die Frage: Wie hoch ist die Cyberresilienz in Europa wirklich?

Vor diesem Hintergrund hat HarfangLab Sapio Research beauftragt, 750 IT-Verantwortliche in ganz Europa zu befragen, um ihren Umgang mit der wachsenden Bedrohungslandschaft zu verstehen. Ziel ist es, ein besseres Verständnis für die Probleme zu schaffen und Sicherheitsverantwortliche genau dort zu unterstützen, wo ihre Unternehmen es wirklich benötigen.

Angesichts der vielfältigen Cyber-Bedrohungen und sinkender Investitionen ist es wichtig, die tatsächlichen Quellen der Risiken zu verstehen und ihnen strategisch zu begegnen. Nur so können Unternehmen ihre Unabhängigkeit, ihren wirtschaftlichen Vorteil und letztlich ihr Überleben sichern.

In diesem Bericht zeigen wir die Prioritäten und Erwartungen der KMU auf, untersuchen einige der Hindernisse für eine bessere Cybersicherheit und beantworten eine zentrale Frage: Wie widerstandsfähig sind europäische KMU gegenüber Cyberrisiken?

EIN HINWEIS ZUR METHODIK

Dieser Bericht basiert auf einer Online-Umfrage, die von Sapio Research im April 2024 durchgeführt wurde. 750 IT-Sicherheitsverantwortliche aus Deutschland, Frankreich, Belgien und den Niederlanden wurden zu ihrer Wahrnehmung und ihrem Bewusstsein für Cyberbedrohungen befragt sowie dazu, wie gut ihre Organisation auf den Umgang mit Cybersicherheitsrisiken vorbereitet ist.

Von den 750 Befragten stammen jeweils 300 aus Frankreich und Deutschland, 100 aus Belgien und 50 aus den Niederlanden. Die Größe der Unternehmen reichte von 300 bis 4.000 Mitarbeitenden.

ÜBER HARFANGLAB

HarfangLab mit Sitz in Paris ist ein europäischer Cybersicherheitsspezialist, der Unternehmen mit seiner KI-gestützten Endpoint-Security-Software-Suite dabei unterstützt, ihre allgemeine Cyberresilienz zu verbessern.

HarfangLab wurde 2018 gegründet und hat sich zum Ziel gesetzt, die Datenbestände von Unternehmen weltweit zu schützen. Das Unternehmen stützt sich auf die Expertise seiner Gründer: Grégoire Germain (CEO) und Xavier Boreau (CFO), Mathieu Gaspard (Head of R&D) und Maxime Rameau (CPO). Sie alle sind Veteranen im Bereich Cybersicherheit mit Erfahrungen im Militär-, Geheimdienst- und Telekommunikationssektor. HarfangLab bietet eine einzigartige Cloud-agnostische Endpoint Detection and Response (EDR)-Softwarelösung an, die Bedrohungen für Unternehmen erkennt, analysiert und neutralisiert und sie so in die Lage versetzt, sich gegen Cyberangriffe zu schützen.

Die Software von HarfangLab gehört zu den weltweit besten EDR-Lösungen, was durch die erstklassigen MITRE ATT&CK-Bewertungen und die EU-Zertifizierung durch die französische Nationale Agentur für Cybersicherheit (ANSSI) belegt wird. Sie bietet eine vertrauenswürdige Option für ihre Nutzer, zu denen mehrere Regierungsbehörden, Unternehmen und internationale Organisationen gehören, die in hochsensiblen Bereichen tätig sind.

EUROPÄISCHE RECHTSVORSCHRIFTEN IM CYBERSICHERHEITSBEREICH BIETEN KLEINEN UND MITTLEREN UNTERNEHMEN EINEN WETTBEWERBSVORTEIL

Die europäische Gesetzeslandschaft für Daten- und Cybersicherheit wird zunehmend komplexer. Neben der bekannten Datenschutz-Grundverordnung (DSGVO) ist in diesem Jahr der European Data Act in Kraft getreten. Später im Jahr wird die NIS-2-Richtlinie wirksam, die die EU-Mitgliedstaaten verpflichtet, strenge Cybersicherheitsvorschriften zu erlassen und konsequent durchzusetzen. Unternehmen der Finanzbranche müssen ab Januar 2025 zudem die Anforderungen des Digital Operational Resilience Act (DORA) erfüllen und angemessene Maßnahmen zum Schutz der Cybersicherheit umsetzen.

Man könnte annehmen, dass europäische KMU die bevorstehenden Compliance-Anforderungen im Bereich der Cybersicherheit als negativ empfinden würden. Doch die Ergebnisse unserer Untersuchung widerlegen dies.

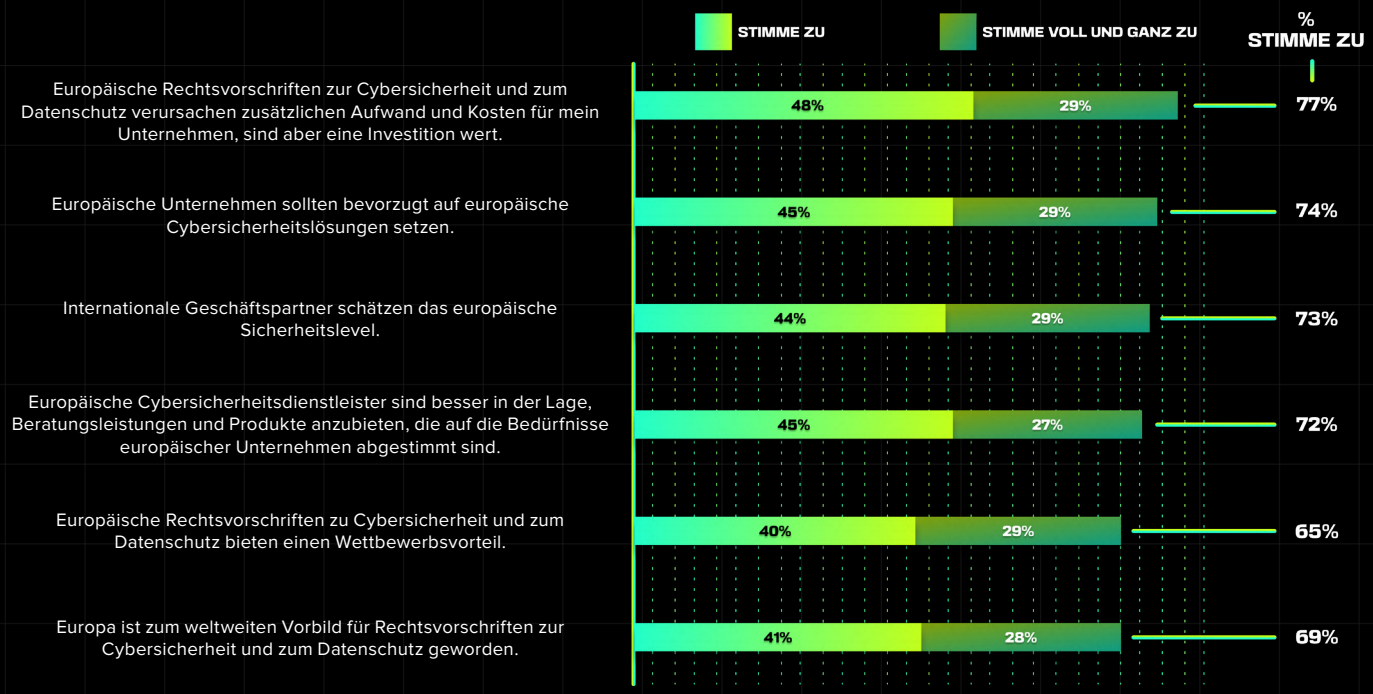
Die Einhaltung der verschiedenen europäischen Rechtsvorschriften zur Cybersicherheit und zum Datenschutz bedeutet für kleine und mittlere Unternehmen zusätzlichen Aufwand und Kosten. Dennoch sind mehr als drei Viertel (77 Prozent) der Befragten der Meinung, dass sich diese Anstrengungen letztendlich auszahlen.

Doch warum? 73 Prozent der befragten IT-Sicherheitsverantwortlichen geben an, dass Geschäftspartner weltweit das hohe Sicherheitsniveau des europäischen Gesetzesrahmens schätzen. Infolgedessen sind 70 Prozent der Befragten der Meinung, dass die europäische Cybersicherheits- und Datenschutzregulierung kleinen und mittleren Unternehmen einen Wettbewerbsvorteil in der globalen Wirtschaft verschafft.

«Es ist eine gute Nachricht, dass die meisten KMU die anstehenden Vorschriften als Chance sehen – denn das sind sie wirklich. Obwohl noch nicht alle Vorschriften in allen Ländern wirksam sind, können sich die Unternehmen doch auf ihren Zweck, die Sicherheit zu erhöhen, vorbereiten. Sicherheit ist kein Prozess, bei dem man nur ein Kästchen auf einer Liste abhakt, sondern eine Kombination aus Menschen, Technologien und Governance. Der wichtigste Rat, den wir Unternehmen im Zusammenhang mit der NIS-2-Richtlinie geben können, ist es, die Führungsebene und die Entscheidungsträger in den Unternehmen einzubinden. Sie sollten sie von der Bedeutung der Cybersicherheit überzeugen und der Tatsache, dass jeder im Unternehmen eine Rolle zu spielen hat. In dieser Hinsicht ist die NIS-2-Richtlinie eine echte Chance für CISOs, um den Rest ihrer Organisation wachzurütteln.»

Anouck Teiller, Chief Strategy Officer bei HarfangLab

77 Prozent geben an, dass europäische Rechtsvorschriften zur Cybersicherheit und zum Datenschutz zusätzlichen Aufwand und Kosten für ihr Unternehmen verursachen, diese Investition aber letztendlich sinnvoll ist.



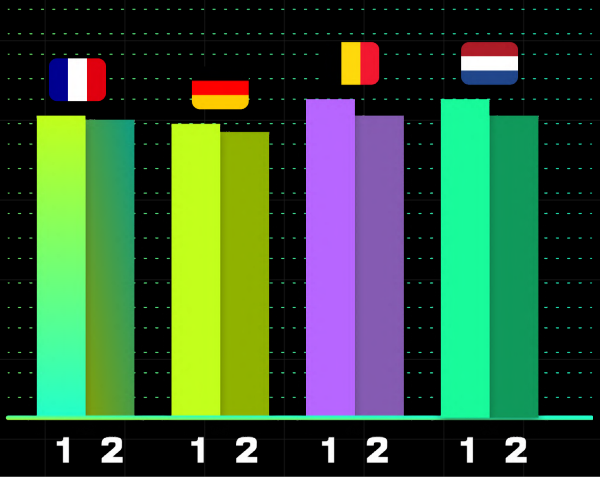
In diesem Punkt gab es kaum Unstimmigkeiten zwischen den Regionen. Tatsächlich sind IT-Sicherheitsverantwortliche aus Deutschland und Belgien (73 Prozent und 74 Prozent) sogar noch mehr als ihre französischen Kollegen (68 Prozent) davon überzeugt, dass die EU-Rechtsvorschriften zur Cybersicherheit und zum Datenschutz einen Wettbewerbsvorteil darstellen. Die niederländischen Befragten waren etwas skeptischer: Nur 50 Prozent stimmen diesem Standpunkt zu. Zugleich sind in jedem Land etwa ähnlich viele Befragte der Meinung, dass sich die Kosten für die Einhaltung der Vorschriften lohnen (Frankreich: 77 Prozent, Deutschland: 76 Prozent, Belgien: 77 Prozent, Niederlande: 82 Prozent).

EUROPÄISCHE CYBERAUTONOMIE BEVORZUGT

Unsere Untersuchung ergab außerdem, dass europäische kleine und mittlere Unternehmen eine Zusammenarbeit mit europäischen Anbietern von Cybersicherheitslösungen bevorzugen.

So sind für 72 Prozent der Befragten europäische Cybersicherheitsanbieter besser in der Lage, sie zu beraten und Produkte zu entwickeln, die den europäischen Bedürfnissen entsprechen. Dabei befürworten fast drei Viertel (74 Prozent), dass sich europäische Organisationen bemühen sollten, überwiegend europäische Cybersicherheitslösungen zu verwenden.

Auch hier gab es kaum Differenzen zwischen den untersuchten Ländern: Alle Regionen unterstützen die Idee, europäische Cybersicherheitspartner zu wählen (Frankreich: 74 Prozent, Deutschland: 72 Prozent, Belgien: 78 Prozent, Niederlande: 78 Prozent). Gleichermaßen sind sie auch davon überzeugt, dass diese ihre Bedürfnisse besser erfüllen können (Frankreich: 73 Prozent, Deutschland: 70 Prozent, Belgien: 74 Prozent, Niederlande: 74 Prozent).



Das könnte daran liegen, dass europäische Anbieter Compliance-Anforderungen in ihre Produkte integrieren. Da sie den gleichen gesetzlichen Vorgaben wie ihre Kunden, den kleinen und mittleren Unternehmen, unterliegen, sind sie außerdem besser in der Lage, Ratschläge und Hinweise zur Einhaltung bestehender und neuer Rechtsvorschriften zu geben. Anbieter aus dem außereuropäischen Ausland, die unter ganz anderen Marktbedingungen und gesetzlichen Rahmenbedingungen arbeiten, können möglicherweise nicht diese gezielte Unterstützung bieten.
Ein weiterer Grund könnte in der Geopolitik liegen: 28 Prozent der Befragten nannten die Zunahme geopolitischer Konflikte als den wichtigsten Faktor, der das Bedrohungsniveau für ihr Unternehmen erhöht. Internationale Ereignisse wie die Olympischen Spiele, die Fußball-Europameisterschaft und die Europawahlen bieten viele Angriffsmöglichkeiten für Bedrohungsakteure.

Aufgrund dieser zunehmenden Spannungen wird die Idee einer souveränen europäischen Cybersicherheitsarchitektur für europäische KMU immer attraktiver. Kleine und mittlere Unternehmen erkennen, dass sie Partner benötigen, die die lokale Bedrohungslandschaft kennen und ihnen helfen können, sich auf alle Eventualitäten vorzubereiten.

«Die heutige Bedrohungslage, verbunden mit geopolitischen und wirtschaftlichen Herausforderungen, unterstreicht die Notwendigkeit, ein widerstandsfähiges Europa im Bereich der Cybersicherheit aufzubauen. Das bedeutet, dass wir Sicherheitsstandards verbessern und unsere Proaktivität erhöhen müssen. Zudem müssen wir in der Lage sein, selbst zu entscheiden, welche Anforderungen wir an den Datenschutz und die Sicherheit stellen, wer auf unsere Daten zugreifen darf und zu welchem Zweck. Angesichts der Entwicklung und Ausweitung extraterritorialer Gesetze und Vorschriften ist diese Fähigkeit von entscheidender Bedeutung. Dies ist der Schlüssel zu Autonomie und Unabhängigkeit. Die gute Nachricht: Es handelt sich hierbei nicht um eine Ideologie. Tatsächlich gibt es bereits Lösungen und technische Antworten auf diese Bedürfnisse.»

Anouck Teiller, Chief Strategy Officer bei HarfangLab

ZEIT FÜR EUROPA ZU HANDELN

Da geopolitische Spannungen mit der steigenden Cyberkriminalität zusammenhängen, stellt sich die Frage: Was sollten kleine und mittlere Unternehmen in Europa dagegen tun?

Zunächst ist es wichtig, den Wert ihrer Daten vollständig zu erfassen und entsprechend eine effektivere Cybersicherheitsstrategie zu entwickeln. KMU bilden den größten Teil der europäischen Wirtschaftslandschaft, weshalb die Verbesserung ihrer Cyberresilienz für das langfristige Wohlergehen des Kontinents entscheidend ist. Obwohl sie denselben Bedrohungen wie große Unternehmen ausgesetzt sind, verfügen sie über deutlich weniger Ressourcen zur Abwehr.

Kein Unternehmen sollte seine Sicherheitserwartungen aufgrund seiner Größe zurückschrauben. Es gibt geeignete Ansätze, um sowohl hochwertige Technologien als auch menschliches Fachwissen bereitzustellen und dabei die Datenhoheit zu berücksichtigen. Der Rückgriff auf europäische Cybersecurity-Anbieter bietet mehr Autonomie und Unabhängigkeit als die Nutzung US-amerikanischer Dienstleister – die ebenfalls anfällig für geopolitische Konflikte oder Cyberangriffe sein können. Die Zusammenarbeit mit vertrauenswürdigen Partnern, die durch einen „Cybersecurity-as-a-Service“-Ansatz maßgeschneiderte Lösungen anbieten, kann eine strategische Methode sein, um interne Personalengpässe zu überwinden. Ein solcher Partner ist nicht nur Experte im Umgang mit den gewählten Technologien, sondern auch mit den Anforderungen des jeweiligen Marktes vertraut. Die entscheidenden Vertrauensmerkmale sind am Ende: Kundennähe, Leistung und Transparenz. Auf die Frage, worauf KMU bei der Suche nach einem IT-Sicherheitsanbieter am meisten Wert legen, antworten sie an erster Stelle Preis-Leistungs-Verhältnis (44 Prozent), Innovation (51 Prozent) und Leistung (44 Prozent), dicht gefolgt von dem „Verständnis für die eigenen speziellen Bedürfnisse“.

Docaposte, die digitale Tochtergesellschaft der La Poste-Gruppe, hat das erste vollständige, sofort einsatzbereite Cybersicherheitsangebot auf den Markt gebracht, das speziell auf die Bedürfnisse und Ressourcen von KMU, lokalen Behörden und Gesundheitseinrichtungen zugeschnitten ist. Dieses Angebot vereint die gesamte Palette an Lösungen zur Prävention, zum Schutz und zur Reaktion über eine einzige Anlaufstelle. Dazu stützt sich Docaposte auf sein Know-how im Bereich der Beratung und die Zusammenarbeit mit einem französischen und europäischen Netzwerk von zwölf Partnerunternehmen, die aufgrund ihres Fachwissens ausgewählt wurden. Auch HarfangLab ist Teil davon und unterstützt Docaposte als globalen EDR-Anbieter.

Dadurch wird die Bedeutung eines einzigen Ansprechpartners hervorgehoben, der sowohl das Ökosystem als auch die Feinheiten des Marktes kennt. Außerdem zeigt es die Herausforderung, eine Vorauswahl vertrauenswürdiger, europäischer und qualitativ hochwertiger Lösungen zu treffen, um eine starke und zugängliche Alternative für europäische KMU zu schaffen.
Investitionen in digitale Technologien und Lösungen sind entscheidend, ebenso wie die Fähigkeit, diese Technologien zu verwalten oder den richtigen Partner dafür auszuwählen. Diese Technologien können einen Wettbewerbsvorteil darstellen und es bestimmten Unternehmen und Branchen ermöglichen, die Marktführung zu übernehmen. Werden sie jedoch von Bedrohungsakteuren genutzt oder unter deren Kontrolle gebracht, können dieselben Technologien die Vereinnahmung ganzer Volkswirtschaften ermöglichen.

Um dieses Spiel nicht zu verlieren, muss Europa proaktiv handeln. Kleine und mittlere Unternehmen in Europa wissen, dass dies einen technologischen Ansatz erfordert, der die strategische Autonomie sowie Unabhängigkeit bewahrt und durch eine starke Governance unterstützt wird.

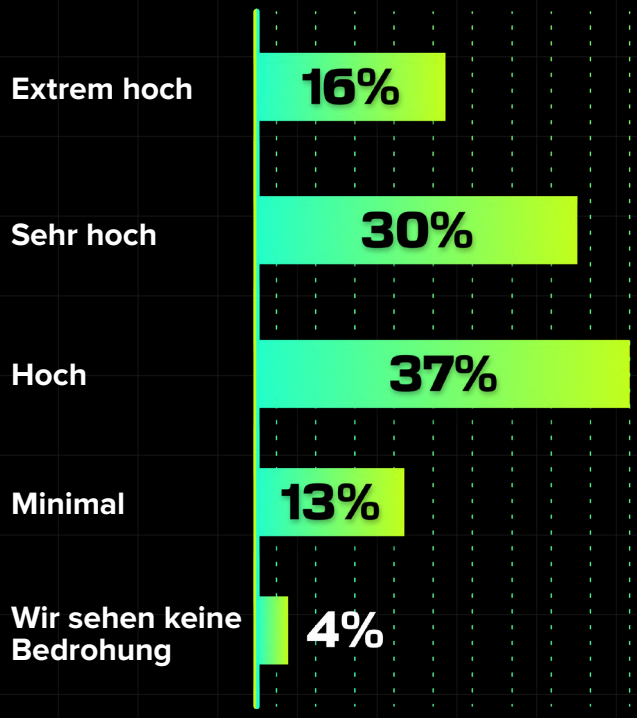
Im nächsten Abschnitt dieses Berichts werden wir untersuchen, wie gut die heutigen KMU auf die aktuelle Bedrohungslage vorbereitet sind und wo sie die größten Risiken sehen.

CYBERRISIKEN: WAHRNEHMUNG, RISIKOFAKTOREN UND VORBEREITUNG

Aufgrund der rasanten Entwicklung der Bedrohungslage wollten wir herausfinden, wie kleine und mittlere Unternehmen in Europa die Gefahren einschätzen, denen sie ausgesetzt sind. Das Ergebnis: Fast die Hälfte der Befragten (46 Prozent) stuft die aktuelle Bedrohungslage als sehr oder extrem ernst ein, während nur drei Prozent behaupten, keiner Bedrohung ausgesetzt zu sein. Dies zeigt, dass die Mehrheit der IT-Verantwortlichen das derzeitige Risikopotenzial durchaus realistisch einschätzt.

Es gibt auch Anzeichen dafür, dass das Ausmaß der Sorgen die entsprechenden Maßnahmen und Investitionen vorantreibt. Die Unternehmen, die angeben, auf einen Vorfall im Bereich der Cybersicherheit vollständig vorbereitet zu sein, stufen die aktuelle Bedrohungslage fast dreimal so häufig als „extrem“ ein (28 Prozent) wie jene ohne gute Vorbereitung (10 Prozent).

Fast die Hälfte (47 %) schätzt das Level an Cyberbedrohungen, dem ihr Unternehmen ausgesetzt ist, als sehr oder extrem hoch ein.



Und wie nehmen die verschiedenen Regionen die Bedrohungslage wahr? In Frankreich wird die Bedrohungslage am höchsten eingestuft: 62 Prozent der Befragten in diesem Land gaben an, dass die Bedrohung sehr oder extrem ernst sei – verglichen mit 38 Prozent in Belgien, 37 Prozent in Deutschland und weniger als einem Viertel (24 Prozent) in den Niederlanden.

Im Branchenvergleich sind Unternehmen im Gesundheitswesen am meisten über das Ausmaß der Cyberbedrohung besorgt: 70 Prozent der Befragten stuften die Bedrohung als sehr oder extrem ernst ein. Es folgten die Bereiche Rechnungswesen und Finanzen (56 Prozent), Fertigung und Einzelhandel/ Großhandel (jeweils 43 Prozent) und schließlich das Bildungswesen (37 Prozent).

Wir fanden außerdem heraus, dass das Bewusstsein für die Cyberbedrohungslage mit der Unternehmensgröße zunimmt. Nur 40 Prozent der Befragten in Unternehmen mit 300 bis 999 Mitarbeitenden stuften die Bedrohungslage als sehr oder extrem ernst ein. Bei Unternehmen mit mehr als 2.000 Mitarbeitenden ist es mehr als die Hälfte (52 Prozent), was eine Differenz von zwölf Prozentpunkten ausmacht.

Auf den ersten Blick mag dies mit allgemeinen Annahmen über Cyberbedrohungen übereinstimmen: Größere Organisationen sind sichtbarer und haben wahrscheinlich mehr Daten sowie finanzielle Ressourcen – und könnten daher eher lohnende Ziele sein – als kleinere Organisationen. In der Realität betreffen Cyberangriffe jedoch alle Arten von Unternehmen, unabhängig von ihrer Größe oder Branche. Kleine und mittlere Unternehmen sind tatsächlich besonders gefährdet: Allein im Jahr 2022 waren sie über 330.000 Angriffen ausgesetzt, deren Folgen bis zur Insolvenz reichen können. Daraus wird deutlich, dass kleinere Unternehmen ihre Cybersicherheit nicht auf die leichte Schulter nehmen sollten. Sie müssen die Bedrohung ernst nehmen.

DER EXPERTENBLICK: DIE VERSCHIEDENEN ARTEN VON CYBERRISIKEN FÜR EINE ORGANISATION

von Léna Jakubowicz, Pre-Sales Engineer bei HarfangLab

Eine Cyberkrise ist eine spezielle Art von Krise, mit der ein Unternehmen konfrontiert werden kann. Die damit verbundenen Risiken sind sehr vielfältig und jedes Risiko hat seine eigenen Konsequenzen. Daher sollte sich ein geeigneter Krisenmanagementplan auf die Aspekte fokussieren, die dem Unternehmen den größten Schaden zufügen könnten.

FINANZIELLE RISIKEN: Colonial Pipeline-Angriff im Jahr 2021. Ein Ransomware-Angriff der DarkSide-Gruppe zwang Colonial Pipeline zur vorübergehenden Schließung seines Pipelinenetzes und beeinträchtigte auch die Kraftstoffversorgung im Osten der Vereinigten Staaten für einige Tage. Es kostete Colonial Pipeline mehr als 4,4 Millionen Dollar an Lösegeld, um den Zugang zu seinen Systemen wiederzuerlangen, zuzüglich der finanziellen Verluste, die durch die anhaltenden Lieferunterbrechungen entstanden waren.

REPUTATIONSRISIKEN: Datenpanne bei Facebook (2021). Persönliche Daten von mehr als 530 Millionen Facebook-Nutzern wurden online veröffentlicht, darunter Telefonnummern und Profilinformationen. Diese Datenpanne warf ernste Fragen zu den Datenschutzverfahren von Facebook auf und beeinträchtigte das Vertrauen der Nutzer und der breiten Öffentlichkeit in die Plattform.

OPERATIVE RISIKEN: Ransomware-Angriff auf JBS (2021). Der weltweit größte Fleischlieferant wurde von einem Ransomware-Angriff getroffen, der JBS zwang, mehrere Produktionszentren zu schließen und die Produktion in Nordamerika und Australien zu stoppen. Dies führte zu einer erheblichen Störung der Fleischlieferkette und beeinträchtigte den Vertrieb.

RECHTLICHE RISIKEN: Datenpanne bei British Airways (2018). Im Jahr 2018 kam es bei British Airways zu einer Datenpanne, bei der die persönlichen Daten von 429.612 Kunden offengelegt wurden. Im Jahr 2020 verhängte die britische Datenschutzbehörde ICO eine Geldstrafe in Höhe von mehreren Millionen Pfund gegen das Unternehmen, nachdem es „mangelhafte Sicherheitspraktiken“ festgestellt hatte. Auch die kommenden europäischen Verordnungen sehen Geldstrafen für Unternehmen vor, wenn sie sich nicht an die Sicherheitsverfahren und -praktiken halten.

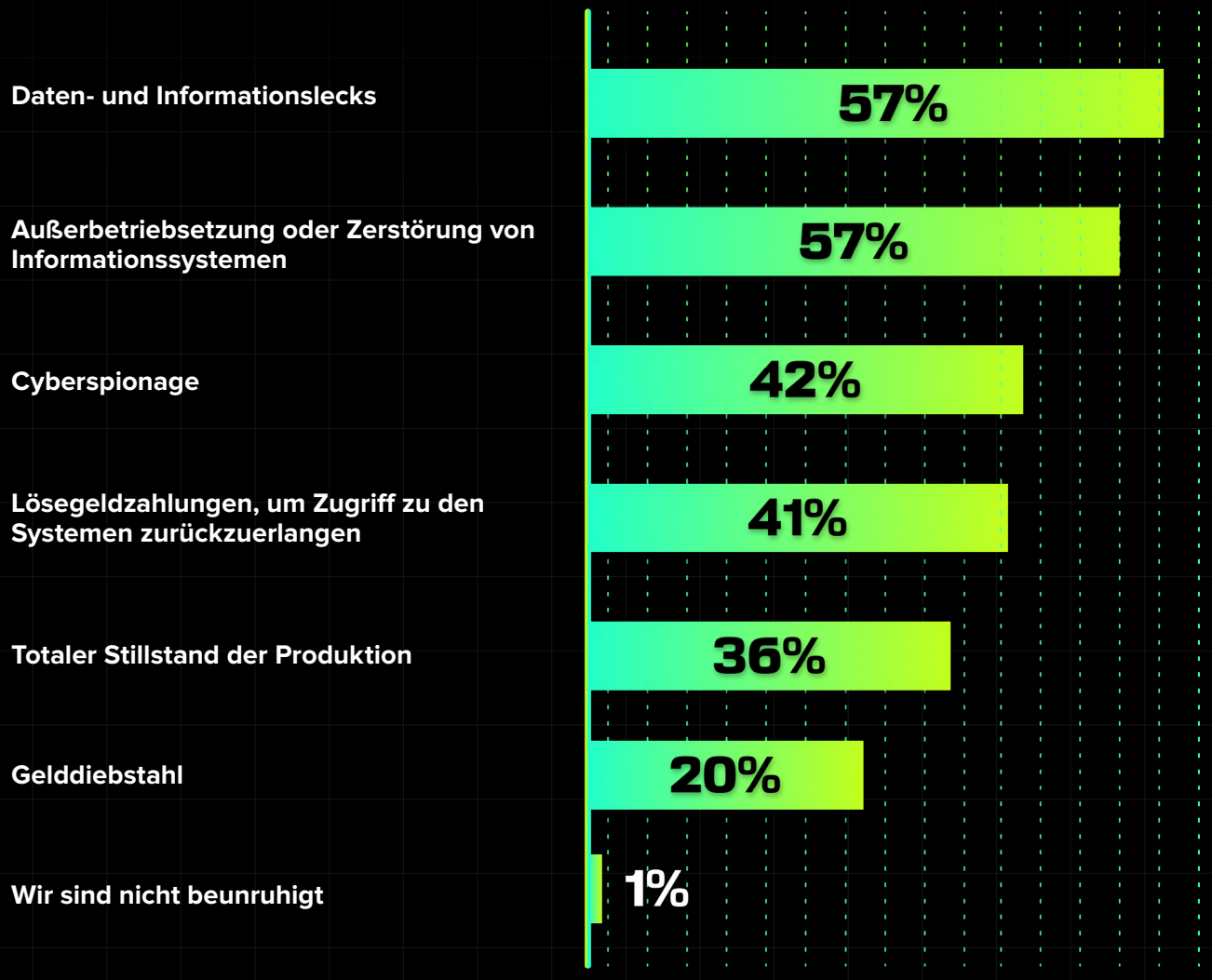
DIE AUSWIRKUNGEN EINES CYBERVORFALLS

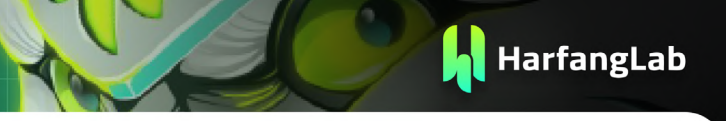
Es ist nicht überraschend, dass praktisch alle Befragten (99 Prozent) angaben, sich Sorgen über die Folgen eines Cyberangriffs zu machen. Doch Cyberangriffe gibt es in vielen Formen und Ausprägungen. Welche bereiten den IT-Entscheidungsträgern die größten Sorgen?

Am wenigsten beunruhigend ist erstaunlicherweise der Diebstahl von Geld: Nur 20 Prozent der Befragten äußerten diese Befürchtung. Das liegt womöglich an den damit verbundenen Schwierigkeiten, einer möglichen Versicherungspolice, die den Verlust abdecken könnte, oder an den Finanzkontrollen, die Unternehmen zum Diebstahlschutz eingerichtet haben.

Dagegen bereiten Daten- und Informationslecks schon 57 Prozent der Befragten Sorgen. Eine Datenpanne kann dem Ruf erheblich schaden und aufgrund von Vorschriften wie der Datenschutz-Grundverordnung möglicherweise zu erheblichen Geldstrafen führen. Ebenso sind mehr als die Hälfte der Befragten (51 Prozent) besorgt darüber, dass ein Cybervorfall ihre Informationssysteme außer Betrieb setzen oder zerstören könnte.

99 Prozent aller IT-Verantwortlichen sind über die möglichen Auswirkungen von Cyberattacken beunruhigt. 57 Prozent von ihnen sind besonders über Daten- und Informationslecks besorgt, weitere 51 Prozent über die Zerstörung von Informationssystemen.





DIE VERNETZTE WIRTSCHAFT VERSCHÄRFT DIE CYBERRISIKEN

Wir wissen nun, welche Folgen ein Cybersicherheitsvorfall für kleine und mittlere Unternehmen von heute hat. Doch wo sehen die IT-Verantwortlichen die größten Risiken, die zu einem erfolgreichen Cyberangriff führen könnten?

Rund die Hälfte der Befragten gab an, dass technische Schwachstellen (56 Prozent) das größte Risiko darstellen. Diese Besorgnis war im Bildungssektor (61 Prozent) und in der verarbeitenden Industrie sowie im Energie- und Versorgungssektor (64 Prozent) am höchsten.

Ein weiteres Risiko ist das Anklicken bösartiger Links oder Dateien durch Mitarbeitende (52 Prozent). Das zeigt, wie wichtig es ist, die Kollegen zu schulen und das Bewusstsein für Cyberbedrohungen im gesamten Unternehmen zu schärfen. Knapp die Hälfte (49 Prozent) sieht außerdem in Schwachstellen von Lieferketten ein erhebliches Risiko. Dies steht auch im Zusammenhang mit einer anderen Frage unserer Untersuchung nach den Entwicklungen, die die Bedrohungslage am stärksten erhöhen.

48 Prozent der Befragten gaben an, dass die vernetzte Wirtschaft der Hauptgrund für die hohen Risiken sei. Viele europäische KMU erkennen auf dem heutigen Markt die potenziellen Vorteile, die sich aus dem Teilen von Daten mit ihren Liefer- und Kundenketten ergeben – das kommende EU-Datengesetz soll den Datenaustausch zwischen Privatunternehmen, Bürgern und dem öffentlichen Sektor erleichtern und fördern. Jede Chance birgt jedoch auch Risiken, und die zunehmend vernetzte Wirtschaft vergrößert die Anzahl der potenziellen Lücken, Schwachstellen und Angriffsmöglichkeiten für Kriminelle. Eine Folge dieser vernetzten Wirtschaft ist, dass IT-Sicherheitsverantwortliche anfangen müssen, über ihre eigene IT-Architektur hinauszuschauen und ihre Partner in ihre Cybersicherheitsstrategien einzubeziehen. Die Absicherung der Wertschöpfungsketten sollte definitiv zu den obersten Prioritäten jedes Unternehmens gehören.

Weitere Risikofaktoren waren eine neue Flut von Endgeräten und der Mangel an Fachkräften (beide von 47 Prozent der Befragten genannt). Der Fachkräftemangel bereitete den Befragten aus Belgien (52 Prozent) und den Niederlanden (56 Prozent) größere Sorgen. Auch die Einzel-/Großhandelsbranche (58 Prozent) stufte diesen Faktor am höchsten ein.

Der Aufstieg der generativen KI wurde von 46 Prozent der Befragten als Risikofaktor genannt. Im Gesundheitssektor war KI sogar der wichtigste Grund für die Erhöhung des Bedrohungsniveaus. Nach Ansicht der europäischen KMU-Führungskräfte wird KI voraussichtlich zu ausgeklügelteren Angriffen führen (81 Prozent). Sie glauben jedoch auch, dass KI ein besseres Verständnis der Bedrohungslandschaft ermöglicht und dazu beiträgt, bessere Sicherheitsstrategien zu entwickeln (85 Prozent) sowie KI-gestützte Angriffe im Allgemeinen abzuwehren (82 Prozent).

> **«Die digitale Welt vernetzt Menschen und Volkswirtschaften wie nie zuvor, schafft aber auch Chancen für Cyberangreifer, auf Kosten von Unternehmen erfolgreich zu sein. Die technologische Entwicklung schreitet viel schneller voran als die Ausbildung und das Fachwissen der Menschen. Wir stehen vor einem internationalen Talentmangel. Daher müssen Sicherheitsinstrumente und -technologien so gestaltet sein, dass sie Experten unterstützen und ihre Effizienz steigern, anstatt eine Qualifikationslücke zu schaffen. Jede Technologie birgt Chancen und Risiken. In der Verteidigungsindustrie sind wir gefordert, unser Angebot auf Grundlage der neuesten Innovationen zu entwickeln, das Bewusstsein zu schärfen und zur globalen Verbesserung der Sicherheitsfähigkeiten beizutragen.»**
>
> Anouck Teiller, Chief Strategy Officer bei HarfangLab

WIE GUT SIND KMU VON HEUTE AUF CYBERRISIKEN VORBEREITET?

IT-Verantwortliche verfügen über ein umfassendes Verständnis über die Bedrohungslandschaft und über die Folgen eines erfolgreichen Cyberangriffs. Sie sind in der Lage, Faktoren zu erkennen, die die Risiken für ihr Unternehmen erhöhen. Doch wie gut sind die europäischen KMU auf zukünftige Cyberangriffe vorbereitet?

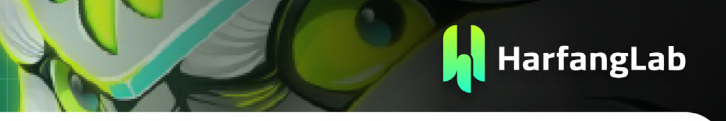
Wenn es um ihre Cybersicherheitsabwehr geht, halten sich derzeit nur 17 Prozent für „vollständig vorbereitet“. Etwa die Hälfte (50 Prozent) hält sich für „sehr gut vorbereitet“, 30 Prozent für „einigermaßen vorbereitet“, und zwei Prozent geben zu, nicht sehr gut vorbereitet zu sein.

In der IT-Branche (32 Prozent), im Gesundheitswesen (28 Prozent) und im Finanzbereich (26 Prozent) sieht sich ein höherer Anteil der IT-Verantwortlichen als „vollständig vorbereitet“. Dies scheint logisch zu sein: IT-Unternehmen sind wahrscheinlich technisch versierter und eher in der Lage, die Bedrohungen zu verstehen, mit denen sie konfrontiert sind. Sie wissen daher auch, welche Schritte sie zum Schutz ihrer Organisation vornehmen müssen. Befragte im Gesundheitswesen sind nach unserer Umfrage am meisten über das Ausmaß der Cyberbedrohungen besorgt. Das hat sie offenbar dazu veranlasst, entsprechende Maßnahmen zu ergreifen und ihre Abwehrstrategien vorzubereiten. Auch die Finanzbranche musste handeln, um die DORA-Verordnung der EU zu erfüllen, die im Januar 2023 in Kraft trat und ab Januar 2025 verbindlich sein wird.

Ebenso fühlen sich international agierende Unternehmen eher „vollständig vorbereitet“ (19 Prozent) als national agierende (15 Prozent).

Doch wie sieht diese Vorbereitung aus? Und welche Schritte können die 83 Prozent der Befragten, die nicht „vollständig vorbereitet“ sind, unternehmen, um ihre Cyberresilienz zu erhöhen? Diesen Fragen werden wir im letzten Abschnitt dieses Berichts nachgehen.

- **ERWARTUNG**: Die Bewältigung von Risiken bedarf einer umfassenden Kenntnis von Informationssystemen, kritischen Vermögenswerten, Daten sowie von Bedrohungen und deren Zusammenhänge. Ein Vorfall im Bereich der Cybersicherheit erfordert dann auch die Fähigkeit, schnell einen Krisenstab einzusetzen, um sowohl technische als auch kommunikative Probleme zu bewältigen.
- **ERKENNUNG**: Für die Aufdeckung von Sicherheitsereignissen sind die richtigen Werkzeuge und Ressourcen erforderlich. Das Informationssystem muss durch geeignete und leistungsstarke Lösungen geschützt werden, die von Fachleuten eingerichtet und verwaltet werden – entweder intern oder mit Hilfe von Partnern.
- **ANALYSE**: Sobald ein Tool ein Sicherheitsereignis erkannt hat, müssen die Experten zur Festlegung der erforderlichen Maßnahmen dessen Schweregrad bewerten und dokumentieren. In dieser Phase geht es auch darum, die Bedrohung und die Ziele des Angreifers zu verstehen, um die bestehende und weitere Ausbreitung zu begrenzen.
- **REAKTION**: Nach der Analyse der Situation können die Experten je nach Kontext die Bedrohung stoppen, Prozesse beenden, Endpunkte isolieren und Dateien unter Quarantäne stellen – mit dem Ziel, das System oder die Daten wiederherzustellen. Zusätzlich zu den technischen Aspekten kann die Reaktionsphase auch interne und externe Kommunikationsmaßnahmen umfassen.
- **BERICHTERSTATTUNG**: Die Analyse nach dem Vorfall ermöglicht es, aus dem Vorfall zu lernen. So kann der Schutz des Informationssystems verstärkt und das Bewusstsein der Benutzer im Hinblick auf künftige Angriffe verbessert werden.



MASSNAHMEN ZUR VERBESSERUNG DER CYBERRESILIENZ

Cyberresilienz ist die Fähigkeit einer Organisation, ihren Kernzweck und ihre Integrität trotz Cyberangriffen und anderer störender Ereignisse aufrechtzuerhalten. Sie geht über herkömmliche Cybersicherheitsmaßnahmen wie Prävention und Verteidigung hinaus und umfasst außerdem die Vorbereitung, Erkennung, Reaktion und Wiederherstellung. Cyberresilienz bedeutet nicht nur Schutz vor Bedrohungen, sondern auch die Fähigkeit, diese schnell zu erkennen, zu mildern und sich an veränderte Umstände anzupassen. Ziel ist es, den Betrieb ohne Unterbrechung fortzusetzen. Technische Lösungen, robuste Prozesse, Mitarbeiterschulungen und eine proaktive Denkweise sind entscheidend, damit eine Organisation Cybervorfälle wirksam bekämpfen und sich von ihnen erholen kann.

Wie widerstandsfähig sind also kleine und mittlere Unternehmen in Europa gegen einen drohenden Cyberangriff? Die meisten KMU (81 Prozent) verfügen über einen Plan für das Krisenmanagement, zugleich haben 80 Prozent sehr großes oder völliges Vertrauen in ihren Plan. Doch nur weniger als ein Drittel würde sich bei der Vorbeugung oder Erkennung (jeweils 27 Prozent), der Reaktion (28 Prozent) oder der Bewältigung (26 Prozent) von Cybersicherheitsvorfällen als „ausgezeichnet“ einstufen. Das Vertrauen in diese Fähigkeiten variiert von Land zu Land. Insgesamt schätzen die Franzosen ihre Fähigkeiten in Bezug auf Cybervorfälle höher ein als ihre Nachbarländer: So bewerten drei Viertel der französischen Befragten (75 Prozent) ihre Fähigkeit, Cyberbedrohungen zu verhindern und zu erkennen, als ziemlich gut oder ausgezeichnet. Was die Budgets für die Cyberverteidigung angeht, so bestätigen mehr als die Hälfte (57 Prozent) der europäischen KMU im Jahr 2024 mehr finanzielle Mittel auszugeben. Nur 17 Prozent geben an, weniger Investitionen zu tätigen. Länder, in denen die Cyberbedrohung als größer eingeschätzt wird, investieren ebenso mehr in die Cybersicherheit: In Frankreich planen 58 Prozent der Befragten, 2024 mehr auszugeben, gegenüber 44 Prozent in den Niederlanden.

Wofür wollen sie diese Budgets ausgeben? Mehr als die Hälfte (52 Prozent) beabsichtigt, in regelmäßige Schulungen zur Sensibilisierung der Mitarbeitenden zu investieren, 50 Prozent werden die Sicherung ihrer Cloud-basierten Systeme und Anwendungen fördern, und 49 Prozent werden sich zu regelmäßigen Audits verpflichten. Von den 17 Prozent der KMU-Führungskräfte, die volles Vertrauen in ihre Verteidigung haben, wollen deutlich mehr in den Aufbau einer Cybersicherheitskultur und -struktur sowie in entsprechende Prozesse investieren (53 Prozent gegenüber 39 Prozent bei den weniger zuversichtlichen Unternehmen). Außerdem geben sie an, ihre Lieferkette schützen zu wollen, was auch die Schulung ihrer Partner einschließt (49 Prozent gegenüber 40 Prozent). Fast alle (93 Prozent) der zuversichtlichen Befragten verfügen auch über einen Plan zur Abwehr von Cyberangriffen, während dies nur 65 Prozent der weniger zuversichtlichen tun.

Doch trotz dieser steigenden Investitionen ist mehr als ein Drittel (35 Prozent) der Befragten der Meinung, dass ihr Budget für Cybersicherheit das Ausmaß der Bedrohung nicht angemessen widerspiegelt. In der Gesundheitsbranche sehen dies sogar 46 Prozent und in der Automobil- und Luftfahrtbranche 58 Prozent der Befragten.

Prävention	**69%**	**75%**	**69%**	**72%**
Erkennung	**65%**	**75%**	**73%**	**66%**
Reaktion	**68%**	**74%**	**72%**	**70%**
Wiederherstellung	**74%**	**72%**	**71%**	**68%**

«Es besteht die weit verbreitete Meinung, dass eine Cybersicherheitsstrategie teuer sein muss, um wirksam zu sein, und dass wir umso besser geschützt sind, je mehr Schutzschichten wir aufbauen. Wir glauben, dass dies nicht unbedingt stimmt. Tatsächlich reicht es oft aus, sich auf die wichtigsten Bedrohungen für das eigene Unternehmen zu konzentrieren und eine solide Grundlage zu schaffen, wie Endpoint Security, Sensibilisierung und IT-Monitoring, So lassen sich die meisten Cyberbedrohungen verhindern. Dabei beobachten wir, dass immer mehr vollständige Cybersecurity-Grundlagen über einen einzigen vertrauenswürdigen Partner, wie Docaposte in Frankreich, auf den Markt kommen.»

Anouck Teiller, Chief Strategy Officer bei HarfangLab

TIPPS ZUM UMGANG MIT EINER CYBERKRISE

Kleine und mittlere Unternehmen können erheblich von der Zusammenarbeit mit einem europäischen Anbieter für Cybersicherheit profitieren, indem er sie bei der Planung zum Umgang mit einer Cyberkrise unterstützt. Eine Möglichkeit hier ist die Wahl eines risikobasierten Managementansatzes. Dieser kann dazu beitragen, die Widerstandsfähigkeit zu erhöhen, die allgemeine Sicherheit zu verbessern und sich in der komplexen Cybersicherheitslandschaft effektiv zurechtzufinden. Zu den Vorteilen eines risikobasierten Managementansatzes gehören:

1 **PROAKTIVITÄT**: Risikobasiertes Management ermöglicht es Organisationen, Cyberrisiken proaktiv zu identifizieren und anzugehen, bevor sie sich zu Krisen entwickeln.

2 **RESSOURCENOPTIMIERUNG**: Durch die Priorisierung von Risiken basierend auf ihrem potenziellen Einfluss können Organisationen ihre Ressourcen effektiver einsetzen und sich zuerst auf die kritischsten Bereiche konzentrieren.

3 **RESILIENZ**: Risikobasiertes Management fördert die Resilienz, indem es Organisationen ermöglicht, Cyberbedrohungen vorherzusehen und zu mindern, wodurch sich die Wahrscheinlichkeit und der Einfluss von Betriebsunterbrechungen reduzieren lassen.

4 **KONTINUIERLICHE VERBESSERUNG**: Durch die Förderung einer Kultur der kontinuierlichen Verbesserung können Organisationen ihre Cybersicherheitsmaßnahmen regelmäßig bewerten und anpassen, um auf sich entwickelnde Bedrohungen und sich ändernde Geschäftsanforderungen zu reagieren.

> **«Es gibt verschiedene Möglichkeiten, Cyberresilienz aufzubauen. Eine davon ist das risikobasierte Management. Das bedeutet, zu akzeptieren, dass eine Cyberbedrohung das eigene Unternehmen wahrscheinlich beeinträchtigen wird, und zu verstehen, dass sich das Risiko durch Maßnahmen zur schnellen Wiederherstellung mindern lässt. Zu diesem Ansatz gehört auch, die eigene Organisation, IT-Infrastruktur und individuelle Bedrohungslandschaft zu verstehen. Organisationen müssen sich darauf konzentrieren, die Risiken, die für sie am schädlichsten sein könnten, zu minimieren oder sogar zu verhindern. Dieser Ansatz kann Ressourcen einsparen und Analysten helfen, sich auf das Wesentliche zu konzentrieren. Der TDIR-Ansatz (Threat Detection, Investigation, Response) ist eine effiziente Strategie für ein risikobasiertes Cybersicherheitsmanagement.»**
>
> Anouck Teiller, Chief Strategy Officer bei HarfangLab

Unternehmen können es sich nicht mehr leisten, beim Schutz ihrer wertvollen Vermögenswerte reaktiv vorzugehen. Durch die Zusammenarbeit mit Cybersicherheitspartnern, die aktiv neue und aufkommende Bedrohungen untersuchen, können sie sich besser darauf vorbereiten und umfassend schützen.

ZUSAMMENFASSUNG

Die Studie zeigt: Unternehmen profitieren am meisten, wenn sie mit Partnern zusammenarbeiten, die sowohl die Bedeutung der Situation verstehen als auch das kulturelle und rechtliche Umfeld in Europa kennen.

Anstatt sich auf externe Anbieter zu verlassen, bevorzugen europäische KMU ihre Autonomie im Cyberbereich. Sie möchten in der Lage sein, Tools und Lösungen innerhalb ihrer eigenen Infrastruktur sowie über die Cloud einzusetzen. Diese Technologien sollten eine Hilfe und kein Hindernis darstellen. Ebenso sollten IT-Verantwortliche die Möglichkeit haben, ihre eigene Vertrauensumgebung aufzubauen und zu entscheiden, wer und was auf die strategischen Daten ihres Unternehmens zugreifen darf.

Wir wissen, dass eine starke Cybersicherheit sowohl Spitzentechnologie als auch menschliche Fähigkeiten und Fachkenntnisse erfordert. Unsere Untersuchung zeigt jedoch auch eine dritte Säule der Cyberabwehr auf: die Gesetzgebung. Die europäischen Vorschriften zur Cybersicherheit und zum Datenschutz verschaffen Unternehmen einen Wettbewerbsvorteil, da sie Kunden und Partnern die Sicherheit ihrer Daten garantieren.

Wissen ist Macht. Europäische KMU müssen verstehen, welche Arten von Bedrohungen sie am ehesten betreffen und wo sie am verwundbarsten sind. Hier kann es ratsam sein, mit europäischen Sicherheitsexperten zusammenzuarbeiten. Diese können speziell auf Europa zugeschnittene Bedrohungsinformationen liefern, was Partner außerhalb des Kontinents möglicherweise nicht in gleicher Weise leisten können.

APPENDIX

CYBERRESILIENZ IN 7 PUNKTEN

Es ist schlichtweg unmöglich, alle Cyberbedrohungen und -vorfälle zu verhindern, so enttäuschend das auch sein mag.

Jede Organisation muss mit der konstanten Bedrohung in der digitalen Welt umgehen. Genau das macht Cyberresilienz zum Schlüssel. Wichtig ist daher, sich darauf zu konzentrieren, die Fähigkeit einer Organisation aufzubauen sowie Störungen zu überstehen, auf sie zu reagieren und sich von ihnen zu erholen, während wesentliche Funktionen und Dienste aufrechterhalten werden.

In einer sich ständig verändernden und herausfordernden Cyberlandschaft hilft dies den Unternehmen und ihren Sicherheitsteams, sich besser zurechtzufinden und sich an die dynamische Natur der Cyberbedrohungen anzupassen. Unserer Meinung nach gibt es hierbei sieben wichtige Punkte zu beachten:

1. VORBEUGUNG UND SCHUTZ

Die eigene Infrastruktur zu schützen ist von entscheidender Bedeutung, um das Risiko von Eindringlingen, Ausspähungen, Datendiebstahl oder Erpressung durch Lösegeldforderungen zu verringern.
Implementieren Sie Tools zur Prävention und zum Schutz vor Cyberbedrohungen, wie EDR, Antivirenprogramme der nächsten Generation, IT-Monitoringtools und Firewalls sowie Maßnahmen wie die Multi-Faktor-Authentifizierung (MFA) und einen Zero-Trust-Ansatz.

Außerdem müssen Sie alle Ihre Lösungen, wie Software, Anwendungen und Betriebssysteme, auf dem neuesten Stand halten, um Schwachstellen zu vermeiden.

Diese Präventions- und Schutzmaßnahmen müssen auch Ihre Zulieferer und Drittanbieter anwenden. Überprüfen Sie, ob sie die bewährten Praktiken und Sicherheitsregeln einhalten, damit sie keine Angriffsfläche für Ihr Informationssystem bieten.

Um im Falle eines Angriffs den Betrieb so schnell wie möglich wiederherzustellen, müssen Sie Ihr Informationssystem genau kennen und Ihre IT-Infrastruktur entsprechend der Wichtigkeit Ihrer Anlagen segmentieren. Die Segmentierung trägt dazu bei, die Auswirkungen eines Angriffs zu begrenzen, da sich die Angreifer nicht seitlich bewegen können. Die Kartierung des Informationssystems hilft, den Ausgangspunkt und die Ausbreitung eines Vorfalls leichter zu erkennen und gegebenenfalls Teile davon zu isolieren.

2. ERKENNUNG UND REAKTION

Wie bereits erwähnt, gehören Investitionen in Ressourcen und aktuelle Technologien zu den Voraussetzungen, um Ihre IT optimal vor den sich ständig weiterentwickelnden Bedrohungen zu schützen.

Dadurch werden Sie in der Lage sein, Vorfälle im Bereich der Cybersicherheit schnell zu erkennen und auf sie zu reagieren. Überwachungs- und Analysetools sowie (interne oder ausgelagerte) Teams helfen, die Bedrohungen umgehend zu untersuchen und zu entschärfen.

Beachten Sie, dass Detection and Response-Tools unverzichtbar und als Teil eines ganzheitlichen Ansatzes noch effizienter sind. Das bedeutet, dass Sie sich auf offene, API-fähige Lösungen verlassen sollten, mit denen Sie Daten über Sicherheitsereignisse sammeln und vergleichen können. Außerdem sollten Sie sich auf Lösungen stützen, die – auch mit Hilfe von KI – sowohl bekannte als auch unbekannte Bedrohungen erkennen können und diese automatisch blockieren.

3. WIEDERHERSTELLUNG UND KONTINUITÄT

Stellen sie Strategien auf, um nach Cybervorfällen ihre Geschäftskontinuität aufrechtzuhalten. Dazu gehören robuste Backup- und Recovery-Prozesse sowie Pläne für die Wiederherstellung kritischer Systeme und Daten, die in einer isolierten und sicheren Umgebung gespeichert werden müssen.

Pläne zu machen, ist schön und gut. Die Pläne müssen jedoch auch regelmäßig getestet werden. Nur so können Sie die wichtigsten Dienste und Tools ermitteln, die Sie im Falle eines Vorfalls als erstes wieder starten, und diejenigen, die Sie möglicherweise abschalten müssen. Es ist auch wichtig zu überlegen, welche Abläufe von Unterbrechungen betroffen sein könnten und wie sich dies auf Ihre Krisenkommunikation und Ihr effektives Krisenmanagement auswirken könnten.

Dieser Ansatz ist entscheidend, um Ihr Informationssystem und Ihr Unternehmen im Falle eines Angriffs so schnell wie möglich wieder zum Laufen zu bringen. Ein IT-Monitoring und die Fähigkeit mit Tools – wie EDR – Daten über die Aktivitäten einer IT-Infrastruktur zu sammeln und zusammenzufassen, erleichtern dies erheblich.

4. ANPASSEN UND LERNEN

Unternehmen sollten sich auf Vorfälle vorbereiten und aus ihnen lernen, sie sollten Richtlinien und Verfahren aktualisieren sowie die Sicherheitslage im Laufe der Zeit verbessern. Mit anderen Worten: Sie müssen ihre Cybersicherheitsmaßnahmen kontinuierlich bewerten und an die sich entwickelnde Bedrohungslandschaft anpassen, was eine ständige Beobachtung neuer Bedrohungen erfordert.

Sie sollten daher in der Lage sein, im Falle eines Angriffs einen Reaktionsplan zu erstellen. Regelmäßige Übungen stellen außerdem sicher, dass Ihre Prozesse richtig sind und dass alle am Krisenmanagement Beteiligten ihre Rollen und Verantwortlichkeiten kennen.

Bei der Bewältigung eines Angriffs ist das Stichwort Agilität. Indem Sie die richtigen Entscheidungen zur richtigen Zeit treffen, können Sie eine schnellstmögliche Wiederherstellung ermöglichen. Dabei gilt es, aus dem Vorfall zu lernen, um den Schutz zu verstärken.

5. KOLLABORATION UND KOMMUNIKATION

Effektive Kommunikationskanäle einzurichten und Rahmenbedingungen zur internen und externen Zusammenarbeit zu schaffen ist für Cyberresilienz unerlässlich. Dies schließt die Koordination zwischen verschiedenen Abteilungen innerhalb des Unternehmens sowie den Austausch von Bedrohungsdaten und bewährten Verfahren mit externen Partnern und Branchenkollegen ein.

Auch das Aufbrechen interner Silos, um die Kommunikation zwischen Sicherheitsteams und anderen Abteilungen zu erleichtern, sorgt für eine bessere und schnellere Reaktion im Falle eines Sicherheitsvorfalls.

Was die externe Kommunikation betrifft, so sollten Sie im Falle eines Angriffs oder Sicherheitsvorfalls eine schnelle, kohärente und transparente Reaktion für Kunden, Presse, Investoren und andere Interessengruppen gewährleisten. Jeder interne Stakeholder muss in der Lage sein zu erkennen, an wen er sich wenden muss, welchen Freigabeprozess die Informationen durchlaufen und über welche Kanäle sie weitergegeben werden müssen.

4. MITARBEITERSCHULUNG UND -BEWUSSTSEIN

Ihre Mitarbeitenden sind entscheidend für die Verhinderung von Social-Engineering-Angriffen und die Aufrechterhaltung der allgemeinen Cyberresilienz. Deshalb ist es wichtig, sie über bewährte Praktiken der Cybersicherheit zu informieren und eine sicherheitsbewusste Kultur im Unternehmen zu schaffen. Laut einer Studie von Thales aus dem Jahr 2023 ist menschliches Versagen nach wie vor die Hauptursache für Datenschutzverletzungen: 31 Prozent der Unternehmen geben dies als Hauptgrund an.

Um ein hohes Maß an Bewusstsein und Wachsamkeit aufrechtzuerhalten, sollten Sie Phishing-Simulationen und regelmäßige Schulungen über die Bedrohungslandschaft durchführen. Cybersicherheit ist ein vielseitiges und faszinierendes Thema, das sich von der Technologie bis zur Geopolitik auf diverse Bereiche anwenden lässt. Sie werden sicher Aspekte finden, die Ihre Teams ansprechen, unabhängig von deren Fachwissen und Sensibilität.

7. GOVERNANCE UND LEADERSHIP

Starke Governance-Strukturen und Richtlinien sowie das Engagement der Führungskräfte müssen auf klaren Rollen und Verantwortlichkeiten, auf Risikomanagementprozessen und auf der Unterstützung durch die oberste Führungsebene aufbauen.

Es ist wichtig, daran zu denken, dass die Cyberkultur von der Spitze des Unternehmens ausgehen muss. Die Entscheidungsträger müssen die Bereitschaft zeigen, das Thema ernst zu nehmen. Unabhängig davon, ob sie es selbst in die Hand nehmen oder andere damit betrauen, müssen sie dem Thema Sicherheit Priorität einräumen. Anstatt das Thema erst im Krisenfall anzugehen, sollten sie es kontinuierlich unter Einbeziehung aller Teams adressieren.

Auch die Einhaltung der gesetzlichen und behördlichen Vorschriften (z. B. NIS-2, DSGVO) spielt eine Rolle, um ein optimales Niveau an vor- und nachgelagerter Sicherheit zu gewährleisten.

Dazu ist es auch wichtig, regelmäßige Sicherheitsaudits durchzuführen. Auf diese Weise können Sie Risiken bewerten und Schwachstellen ermitteln, die Angreifer ausnutzen könnten, um so die Prioritäten für IT- und Sicherheitsteams festzulegen.

Ebenso ist ein Verständnis für die Bedrohungen, mit denen die Organisation konfrontiert ist, von entscheidender Bedeutung. Sie müssen wissen, gegen welche Risiken sie sich schützen müssen, um im Bedarfsfall mit den entsprechenden Ressourcen reagieren zu können.

harfanglab.io Inside the Lab @harfanglab HarfangLab

PRESSEKONTAKT

Noémie Minster
PR & Communications Manager
noemie.minster@harfanglab.fr