CompTIA

State of Cybersecurity 2024

DACH

STATE OF CYBERSECURITY 2024: DACH-REGION

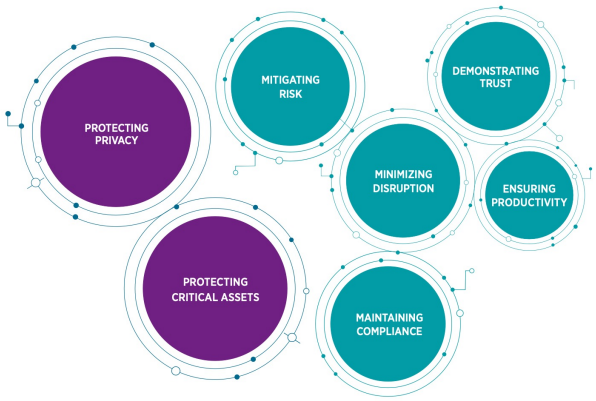
Überblick

Cybersicherheit ist ein ständiger Balanceakt. Seit Jahren gibt es einen Zielkonflikt zwischen Sicherheit und Bequemlichkeit. Sowohl im geschäftlichen wie auch im privaten Umfeld gehen strengere Sicherheitskontrollen oft mit einem geringeren Grad an Bequemlichkeit einher, ein Kompromiss, den die meisten Endnutzer nur ungern eingehen. Unternehmen können das Problem mit Technologie und Richtlinien erzwingen, dies kann jedoch Tür und Tor für riskante Ausweichlösungen öffnen.

Nun kommt eine neue Herausforderung hinzu. Für Chief Information Security Officer (CISOs), Chief Information Officer (CIOs) und andere, die die Unternehmenssicherheit gewährleisten müssen, hat der Konflikt weniger mit Bequemlichkeit, sondern mit Fortschritt zu tun. Während Unternehmen die digitale Transformation vorantreiben und Technologie enger mit dem Geschäftserfolg verknüpfen, können zu restriktive Cybersicherheitsmaßnahmen den allgemeinen Fortschritt behindern. Zu laxe Maßnahmen hingegen, können zu schwerwiegenden Vorfällen führen, die den Fortschritt potenziell beeinträchtigen.

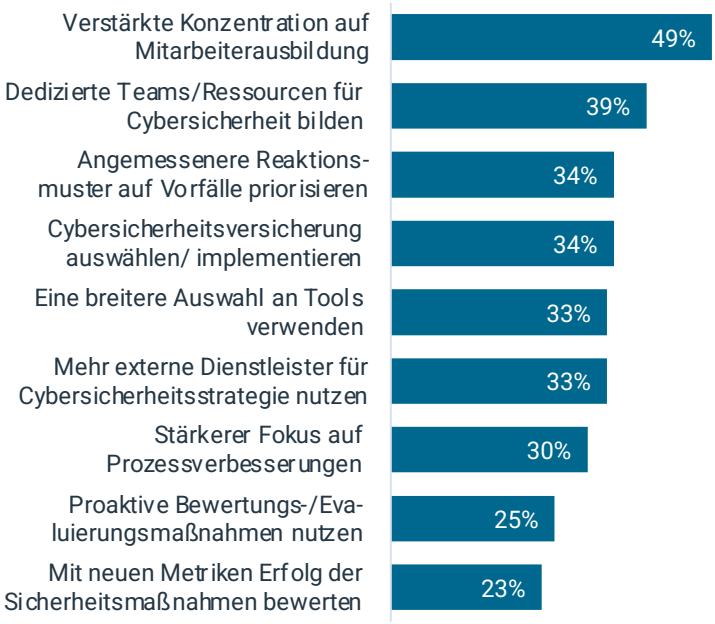
Die CompTIA-Studie „2024 State of Cybersecurity“ untersucht die vielen Faktoren, die beim Abwägen der Gleichung der „Cybersicherheit“ berücksichtigt werden müssen. Da Cybersicherheit zu einer geschäftskritischen betrieblichen Notwendigkeit geworden ist, muss jeder Prozess auf potenzielle Schwachstellen hin untersucht werden. Diese Risikoanalyse dient dann als Grundlage für Entscheidungen über Arbeitsabläufe, den Aufbau von Qualifikationen für Mitarbeiter und die Einführung von Technologien. Indes: die Technologie entwickelt sich genauso weiter wie die Angriffsmuster, was dazu führt, dass ein echtes Gleichgewicht unmöglich zu erreichen ist. Dieser Balanceakt ist daher ein Vollzeitjob.

Zielsetzungen für die Cybersicherheit



Wie schwierig es ist, die richtige Balance zu finden, zeigt ein Blick auf die Ziele hinter den Cybersicherheitsstrategien der Unternehmen. Sechs Regionen beteiligten sich an der CompTIA-Studie „2024 State of Cybersecurity“-Studie, die unterschiedliche wirtschaftliche und technische Reifegrade repräsentieren. In allen sechs Regionen stehen Schutz und Sicherheit an oberster Stelle der Cybersecurity-Strategien, egal ob es um kritische Unternehmensressourcen oder die Privatsphäre von Kundendaten handelt.

Cybersicherheits-Trends im letzten Jahr



Um die Cybersicherheit in den Griff zu bekommen, bedarf es eines vielschichtigen Ansatzes. Das beginnt mit Überlegungen und Maßnahmen, die Prozesse im gesamten Unternehmen verbessern sollen, insbesondere Reaktionen auf Vorfälle. Qualifikationslücken müssen abgebaut werden, sei es durch eine umfassende Ausbildung der Mitarbeiter, spezielle Ressourcen für die Cybersicherheit, externe Partner oder eine Kombination aus allen dreien. Der Werkzeugkasten muss erweitert werden mit gezielter Technologie für spezifische Aktivitäten und Dashboards, die all diese Maßnahmen auf einen Blick zeigen.

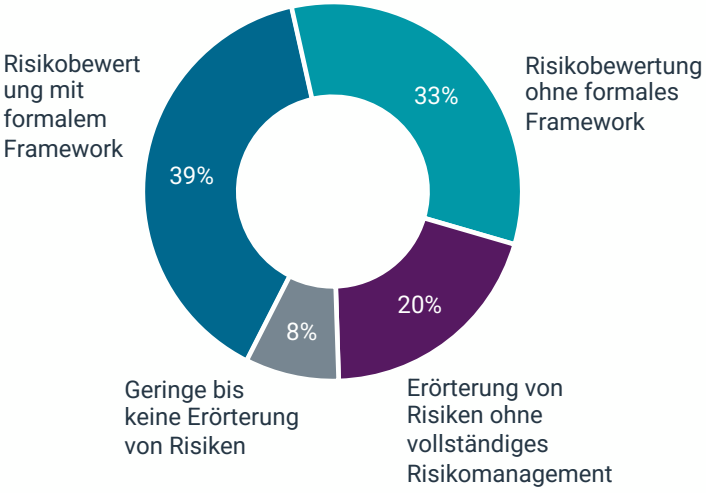
In Bezug auf die Cybersicherheit der Unternehmen in der DACH-Region insgesamt, sind 64 Prozent der Befragten der Meinung, dass sich die Situation verbessert. Organisatorisch gesehen halten 69 Prozent die Cybersicherheit in ihrem Unternehmen für zufriedenstellend. Davon halten 21 Prozent die Situation für voll zufriedenstellend.

Es gibt aber noch viel zu tun. Unternehmen sehen Cybersicherheit vermehrt als kritische Funktion, eng mit der Technologie verflochten, aber auch für sich allein stehend und mit erfolgsrelevanten Kennzahlen. In der nächsten Phase muss der Betrieb dieser eigenständigen Einheit etabliert und verfeinert werden, um mit strategischen Ansätzen taktische Maßnahmen in Bezug auf Personal und Produkte zu steuern.

RISIKOMANAGEMENT UND PROZESSE

In den letzten Jahren ist Risikomanagement eine immer wichtigere Komponente der Cybersicherheit geworden, blieb aber eine Taktik neben anderen, während Unternehmen ihren übergeordneten Ansatz entwickelten. Risikomanagement wird jedoch immer mehr zur Hauptmethode zum Lösen einer der größten Herausforderungen der modernen Cybersicherheit: Die Verbindung zwischen Sicherheitsmaßnahmen und Geschäftsprozessen.

Wie wird das Risikomanagement organisiert?



Die überwältigende Mehrheit der Unternehmen in der Umfrage hat zumindest einige Diskussionen zum Risikomanagement geführt. In manchen Fällen dienen diese Diskussionen im Wesentlichen dazu, das Bewusstsein zu schärfen, und helfen kleinere Unstimmigkeiten über Cybersicherheitsinitiativen zu überwinden. Ein Drittel verfolgt einen ernsthafteren Ansatz und bewertet die Risiken im gesamten Unternehmen, ohne einen formellen Rahmen (Framework) fürs Risikomanagement. Nahezu vier von zehn befragten Firmen verfolgen einen innovativen Ansatz, indem sie eine Art Framework verwenden, um Risiken und damit verbundene Ausgaben zu ermitteln und zu managen.

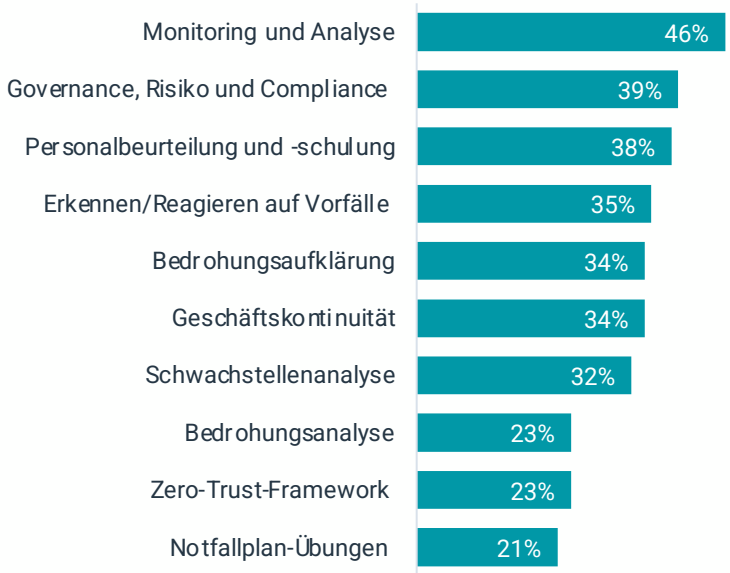
Einer der besten Gründe für die Verwendung eines formellen Rahmens ist, dass er Bereiche identifiziert, die außerhalb der herkömmlichen IT-Systemarchitektur liegen. Viele Interessengruppen nehmen die in der CompTIA-Umfrage vorgestellten Themen gut an. Die Cloud und die Nutzung mobiler Endgeräte sind Standardthemen, während Unternehmen weiter neue IT-Architekturmodelle einführen. Cybersecurity-Profis können Prozesse außerhalb ihrer direkten Zuständigkeit beeinflussen. Das gilt z.B. für die Art der Nutzung von sozialen Medien und die Abläufe, wenn Mitarbeiter ein Unternehmen verlassen.

Je wichtiger den Unternehmen die Verfahren und Prozesse ihrer Cyber-Sicherheitsstrategie sind, desto mehr erkennen sie, dass Cybersicherheit weit über direkte Fragen der Umsetzung von Sicherheitsmaßnahmen hinausgeht.

Risikomanagement umfasst sowohl die Organisation von Prozessen als auch die Integration der Cybersicherheit in Geschäftsabläufe als Grundlage für viele funktionale Entscheidungen.

Cybersicherheit spielt eine wichtige Rolle bei der Bewertung neuer Technologien. Viele Sicherheitsexperten standen im letzten Jahrzehnt oft vor der Herausforderung, mit der Einführung neuer Technologien für die Digitalisierung Schritt zu halten. Unternehmen wollen Technologien schneller einführen, um einen strategischen Vorteil zu erlangen. Cybersecurity-Bedenken stehen dabei nicht immer an erster Stelle.

Wie wird die Cybersicherheit organisiert?



Neben der Einführung von Technologie, weisen auch andere Elemente der Cybersicherheitsstrategie darauf hin, wie sich die Cybersicherheit auf den Geschäftsbetrieb auswirkt. Zum Beispiel geht es bei der Bedrohungsanalyse nicht mehr nur um Viren oder Malware. Neue Arten von Bedrohungen wie Social Engineering und Ransomware verdeutlichen die Überschneidung von IT-Systemen und realen Gegebenheiten.

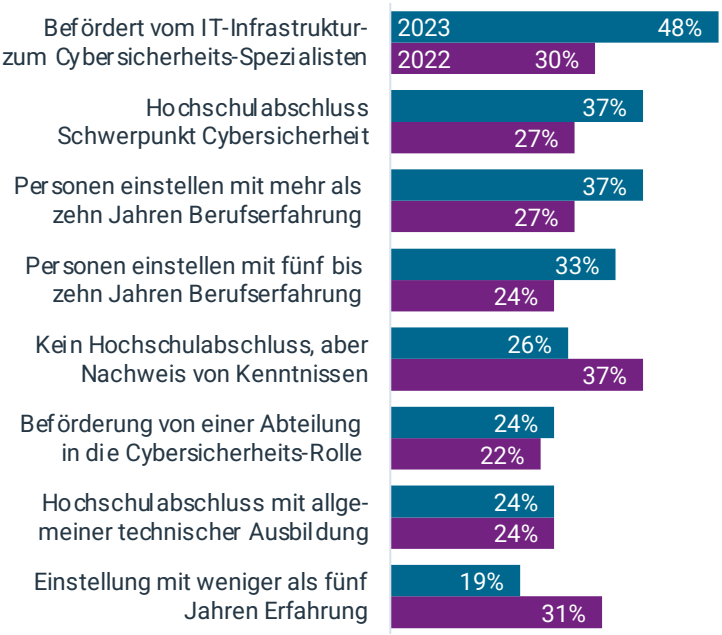
Governance, Risiko und Compliance (GRC) stellen ein weiteres Beispiel dar. In der Vergangenheit galt diese Spezialisierung vor allem für stark regulierte Branchen. Heute muss jedes Unternehmen, unabhängig von Größe und Branche, seine Geschäftsabläufe viel bewusster gestalten. Grund dafür ist das komplexe Geflecht von Vorschriften, die das digitale Geschäft regeln.

Jeder Cybersicherheitsprozess, ob direkt oder indirekt, zielt darauf, sich an den Grundsätzen eines Zero-Trust-Frameworks auszurichten. Auf einer übergeordneten Ebene ist ein Zero-Trust-Framework einfach zu definieren: jede Transaktion wird hierbei durch eine zusätzliche Überprüfungsebene ergänzt, anstatt dass nur auf die einzelnen Komponenten vertraut wird. In der Praxis werden die Details noch komplizierter. Viele Unternehmen setzen jedoch nur auf einzelne Zero-Trust-Prinzipien wie softwaredefinierte Mikrosegmentierung oder Multi-Faktor-Authentifizierung, ohne unbedingt einen umfassenden Zero-Trust-Ansatz zu verfolgen.

TALENTFÖRDERUNG UND EINFLUSS DER KI

Unternehmen haben erkannt, wie wichtig Cybersecurity-Qualifikationen für ihre Mitarbeiter sind. In den letzten Jahren hat sich ein Trend zur Spezialisierung verstetigt. Unternehmen haben Teams von engagierten Cybersicherheits-Experten aufgebaut, anstatt sich auf IT-Generalisten zu verlassen, bei denen die Cybersicherheit nur ein Teil der allgemeinen Stellenbeschreibung ist.

Karrierewege zum Cybersicherheits-Experten



Auf der Suche nach starken und nachhaltigen Teams stellen Unternehmen verstärkt weniger erfahrene Cybersicherheits-Experten ein, die ihre Qualifikationen nach und nach ausbauen und gleichzeitig mit der Unternehmenskultur und den Zielen vertraut werden. Die erste Wahl für den Teamaufbau im Jahr 2023 waren Infrastrukturspezialisten, die ihre Kompetenzen um Cybersecurity ergänzen, sowie Hochschulabsolventen mit einem speziellen Cybersecurity-Fokus.

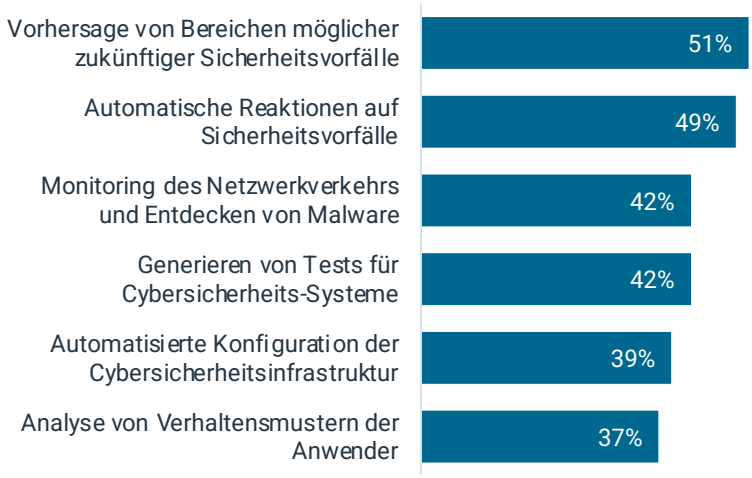
Welche Produkte verwenden diese Fachleute? Ein Trend zieht die Aufmerksamkeit der IT-Mitarbeiter wie der Unternehmensleiter auf sich: die generative künstliche Intelligenz (KI). Tatsächlich halten viele diese neue Welle der KI, die auf großen Sprachmodellen (LLMs) basiert, für den größten technologischen Paradigmenwechsel seit Jahrzehnten. Die Möglichkeiten sind aufregend, aber wie bei den meisten Trends ist die Situation komplizierter, als dass sie über Nacht zum Erfolg führt.

Zum Hintergrund: Generative KI sollte als ein Schritt in der allgemeinen Entwicklung der KI gesehen werden. Es mag ein sehr bedeutender Schritt nach vorn sein, aber viele Unternehmen haben bereits seit geraumer Zeit KI in ihre Arbeitsabläufe integriert.

Über ein Drittel der Unternehmen in der CompTIA-Umfrage (39 Prozent) geben an, dass sie bereits mit KI und maschinellem Lernen (ML) arbeiten.

Die generative KI hebt diese Arbeit auf eine neue Ebene. Darüber hinaus geben 42 Prozent an, dass sie noch nie mit KI/ML gearbeitet haben, sich aber jetzt ernsthaft mit generativen KI-Tools auseinandersetzen. Dies zeigt, wie verlockend die Versprechungen dieser neuen Technologie sind.

Mögliche Einsatzfelder der KI für Cybersecurity



Unternehmen sehen ein breites Spektrum von Einsatzfeldern für die KI in den nächsten zwei bis drei Jahren, was das Potenzial dieser Technologie unterstreicht. Viele der aufgelisteten Verhaltensweisen gibt es bereits heute, sie ergänzen aber neuerdings das Repertoire der Cybersicherheit. Ein Beispiel ist die Analyse von Verhaltensmustern der Nutzer, anstatt sich auf den autorisierten Zugang zu sicheren Perimetern zu verlassen. Für Unternehmen wird es immer schwieriger, neue Funktionen hinzuzufügen, ohne eigene Ressourcen zu erhöhen. Sie werden mit der KI als Tool die wachsende Komplexität bewältigen wollen.

Andere potenzielle Verwendungszwecke sind eher neu. Das gilt für die Vorhersage von Bereichen in denen Sicherheitslücken auftreten könnten oder für Tests der Sicherheits-Systeme. Sie nutzen die Leistungsfähigkeit der KI, um verborgene Muster zu erkennen. In diesen Fällen hilft die KI, neue Wege zu beschreiten und bietet Lösungen mit Hilfe intensiver Berechnungen großer Datensätze und komplizierter mathematischer Modellierung.

Natürlich ist es mit der KI wie mit anderen neuen Technologien: Sie ist nicht eigenständig, sondern kommt eingebettet in andere Produkte daher. Der Werkzeugkasten für die Cybersicherheit hat sich in den letzten Jahren stetig erweitert. Weil KI-Funktionen in jedes einzelne Tool integriert werden, wird, was jetzt schon eine Herausforderung ist, noch komplexer: das Managen zahlreicher Sicherheits-Tools.

Wenn es einen Balanceakt zwischen idealer Cybersicherheit und produktiven Geschäftsabläufen gibt, ist das Erreichen dieses Gleichgewicht, zu einer hochspezialisierten Fähigkeit geworden. Jede Abteilung eines Unternehmens trägt eine gewisse Verantwortung für die Cybersicherheit. Doch nur wer über die richtige Ausbildung und das entsprechende Fachwissen verfügt, kann alle Teile zu einer Lösung mit minimalem Risiko zusammenfügen.

METHODIK

ÜBER DIESE STUDIE

Die „State of Cybersecurity“-Studie von CompTIA liefert Einblicke in die wichtigsten IT-Sicherheits-Trends.

Für die quantitative Studie in der DACH-wurden im Juli 2023 in einer Online-Umfrage IT-Experten und Mitarbeiter aus verschiedenen Geschäftsbereichen befragt. Insgesamt nahmen 132 Personen an der Umfrage teil, was einen Gesamtstichprobenfehler von +/- 8,7 Prozentpunkten bei einem Konfidenzintervall von 95 Prozent ergibt. Der Stichprobenfehler ist bei Untergruppen der Daten größer.

Wie bei jeder Erhebung ist der Stichprobenfehler nur eine mögliche Fehlerquelle. Der Nicht-Stichprobenfehler kann zwar nicht genau berechnet werden, in allen Phasen – von der Fragebogenerstellung, über die Datenerhebung bis hin zu deren Verarbeitung – wurden Vorsichtsmaßnahmen getroffen, um ihn zu minimieren.

CompTIA ist für den gesamten Inhalt und die Analyse verantwortlich. Fragen zur Studie richten Sie bitte an Mitarbeiter von CompTIA Research and Market Intelligence unter research@comptia.org.

CompTIA ist Mitglied der Insights Association der Marktforschungsbranche und hält sich an deren international angesehenen Normen- und Ethik-Codex.

ÜBER COMPTIA

Die Computing Technology Industry Association (CompTIA) ist eine führende Organisation und Fürsprecherin des globalen IT-Ökosystems im Wert von 5 Billionen US-Dollar und der geschätzten 75 Millionen IT- und Industriefachkräften, die die Technologie, welche die Weltwirtschaft antreibt, entwickeln, implementieren, verwalten und schützen. Durch Community, Aus- und Weiterbildung, Zertifizierung, Interessenvertretung, Philanthropie und Marktforschung ist CompTIA die Drehscheibe für die Erschließung des Potenzials der Tech-Branche und ihrer Arbeitskräfte.

CompTIA ist die weltweit führende herstellerunabhängige IT-Zertifizierungsstelle mit mehr als drei Millionen Zertifizierungen, die erreicht werden, wenn man leistungsorientierte Prüfungen besteht. In 232 Ländern auf der ganzen Welt arbeiten Menschen, die CompTIA-Zertifizierungen erworben haben.

CompTIA setzt den Standard für die Ausbildung von Berufsanfängern bis hin zu Experten, die in allen Phasen ihrer Karriere in der IT-Branche erfolgreich sein wollen. Über den philanthropischen Arm von CompTIA entwickelt CompTIA innovative Einstiegsmöglichkeiten und Karrierewege, um die Chancen von Bevölkerungsgruppen zu vergrößern, die in der Informationstechnologie traditionell unterrepräsentiert sind.