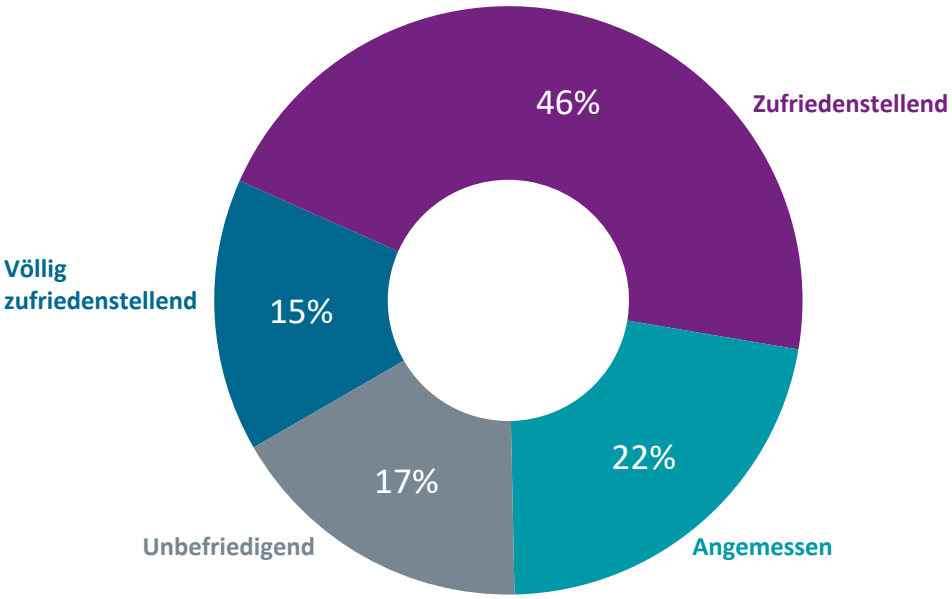
STAND DER CYBERSICHERHEIT 2022: DEUTSCHLAND

Im vergangenen Jahr hat die Geschäftswelt ihre Lehren aus der COVID-Pandemie gezogen. Auf Belegschaftsebene fällt es Unternehmen schwer, die besten Möglichkeiten zu finden, um die Flexibilität der Mitarbeiter und die Unternehmenskultur in Einklang zu bringen. Auf technischer Ebene werden die vielen Vorteile einer Cloud-First-Architektur gegen die Herausforderungen beim Management von Komplexität und Kosten in einer Multi-Cloud-Umgebung abgewogen. Es wird noch Jahre dauern, bis wir verstehen, wie das Gleichgewicht in der Zeit nach der Pandemie aussieht, aber die frühen Veränderungen deuten auf eine erhebliche Umstrukturierung hin.

Eine weitere markante Erkenntnis aus der Pandemie ist, dass Symptome oft leichter zu diagnostizieren und zu behandeln sind als Grundursachen. Dies hat natürlich Auswirkungen jenseits von Unternehmensstrategien, aber ein Paradebeispiel für dieses Konzept in der Geschäftswelt ist der Bereich der Cybersicherheit. Unternehmen werden nur allzu deutlich auf die unzureichende Cybersicherheit aufmerksam, wenn sie verletzt wird, und eine nachträgliche Analyse kann Prozesse oder Tools identifizieren, die den Angriff verhindert oder gemildert hätten. Aber dies geht möglicherweise nicht die zugrundeliegenden Probleme an, die später zu einem anderen Cybervorfall führen können.

Der Bericht über den Stand der Cybersicherheit 2022 von CompTIA untersucht die Trennung zwischen Ursache und Symptomen. Die digitale Transformation, die durch die Einführung der Cloud und des Mobilfunks vorangetrieben wird, zwingt zu einem neuen strategischen Ansatz für die Cybersicherheit. Aber die vollständige Übernahme dieses neuen Ansatzes stellt sowohl taktisch als auch finanziell erhebliche Herausforderungen dar. Wenngleich Cybersicherheit nach wie vor eines der drängendsten Probleme für einen modernen Betrieb ist, erschweren die Hürden, die sich aus den älteren Ansichten der IT und dem geringen Verständnis der Bedrohungsszenarien ergeben, die Umsetzung der verordneten Verfahren.

Zufriedenheit mit der Cybersicherheit in Unternehmen



INTEGRATION EINES ZERO-TRUST-ANSATZES

In vielerlei Hinsicht ist der Bereich der Cybersicherheit eine Reaktion auf die Art und Weise, wie sich Enterprise IT entwickelt. Schließlich kommt der Bedarf an Cybersicherheit erst nach der Implementierung von Technologie. Diese Dynamik hat sich in den letzten Jahren verstärkt, da Unternehmen aggressiv nach Technologien streben und dazu tendieren, Cybersicherheit als zweitrangig zu behandeln.

Eine Art, wie Cybersicherheit die Entwicklung von Enterprise IT widerspiegelt, besteht darin, dass beide strategischer geworden sind. Wenn es um die allgemeine IT geht, akzeptieren Unternehmen im Allgemeinen den Übergang zu einem strategischeren Ansatz, selbst wenn es einige Anfangsschwierigkeiten dabei gibt. Auf der anderen Seite stellt Cybersicherheit eine größere Herausforderung dar, wenn es darum geht, eine strategische Denkweise anzunehmen.

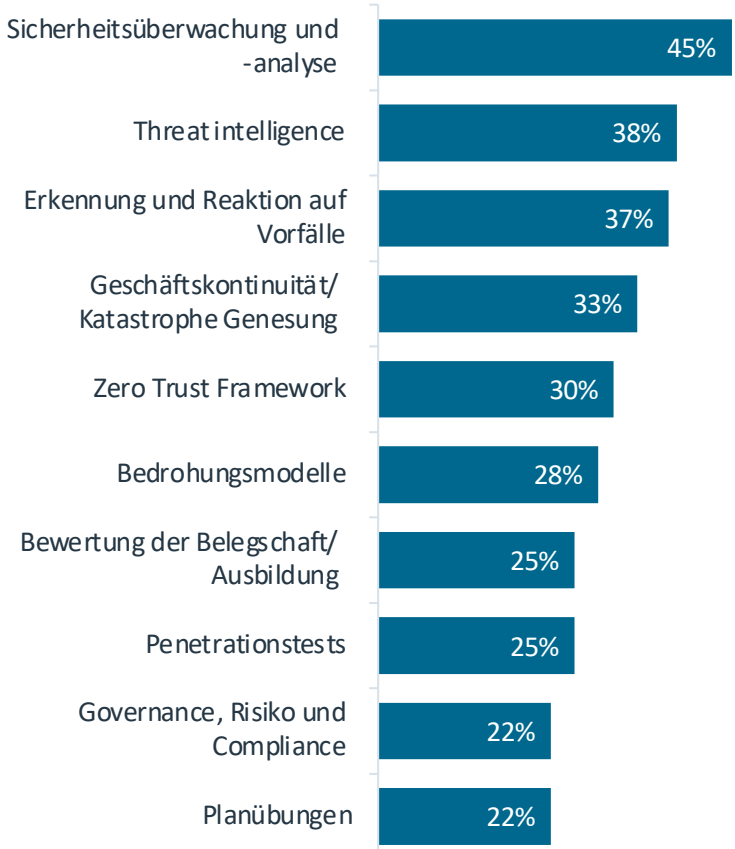
Einer der wichtigsten Bestandteile einer strategischen Denkweise ist die Erkenntnis, dass Cybersicherheit nicht mehr in erster Linie auf externe Ereignisse ausgerichtet ist. Bei der Untersuchung der Probleme, die die Cybersicherheit ankurbeln, sind die meisten der wichtigsten Probleme, die genannt werden, solche, die nach draußen verweisen. Der Fokus auf Volumen, Vielfalt oder Ausmaß der Angriffe ist ein Fokus auf Dinge, die außerhalb des Betriebs passieren. Selbst Bedenken in Bezug auf den Datenschutz sind Bedenken, bei denen es sich um externe Erwartungen dreht. Es wird weniger anerkannt, dass die Cybersicherheit mit dem sich wandelnden Charakter interner Vorgänge verbunden ist, wie etwa einer zunehmenden Abhängigkeit von Daten oder der Notwendigkeit, sich ändernde Vorschriften stets einzuhalten.

Im Laufe des nächsten Jahres wird es einen konzentrierten Schritt hin zur Integration der Cybersicherheit in den Geschäftsbetrieb geben. Die Akzeptanz von Cybersicherheit als wichtiger Bestandteil der digitalen Transformation wird im gesamten Unternehmen zu neuen Fragen führen und neue Erfolgsmaßstäbe setzen. Gleichzeitig wird die Übernahme eines ganzheitlichen Standpunkts viele der bestehenden Hürden um die Änderung des Ansatzes zur Cybersicherheit angehen.

Die Einführung von Cloud Computing und mobilen Geräten veränderte drastisch die Sichtweise eines sicheren Umkreises, die seit Jahrzehnten die vorherrschende Denkweise war. Während sich Unternehmen mit dem Paradigmenwechsel auseinandersetzten, bestand die Schwierigkeit teilweise darin, einen umfassenden Ansatz zu definieren, der ein breites Spektrum von Entscheidungen hinsichtlich der Cybersicherheit prägte. Als Antwort auf dieses Dilemma entstand Zero-Trust.

In diesem Jahr beginnt sich Zero-Trust von einem weit gefassten Ansatz zu taktischen Prozessen zu wandeln. Die Einführung von Zero-Trust erfolgt aus mehreren Gründen nicht von heute auf morgen. In erster Linie stellt Zero-Trust eine völlig andere Denkweise über Cybersicherheit dar. Anstatt Cybersicherheit als eine von vielen Komponenten innerhalb der IT-Funktion zu betrachten und einfach in Hardware oder Software zu investieren, müssen Unternehmen Cybersicherheit jetzt als unternehmerische Notwendigkeit sehen, die sich über Technologieprodukte hinaus auf Entscheidungen über Arbeitsabläufe und Arbeitskräfte erstreckt.

Bestehende Cybersicherheitspraktiken



Zero-Trust ist nicht ein einzelnes Produkt oder eine einzelne Maßnahme. Viele unterschiedliche Tools und Praktiken können Teil eines Zero-Trust-Ansatzes sein. Wenn man Komponenten, die typischerweise unter einen Zero-Trust-Schutz fallen, betrachtet, deuten unterschiedliche Akzeptanzniveaus auf die Durchführbarkeit eines stückweisen Ansatzes hin. Mehrstufige Authentifizierung ist eines der besten Tools zur Überprüfung der vertrauenswürdigen Identität. Sie wird von 26 % der Unternehmen genutzt. Cloud-Workload-Governance, ein Prozess, der sicherstellt, dass Cloud-Ressourcen planmäßig verwendet werden, wird von 28 % der Unternehmen genutzt. Weitere Elemente, wie die software-definierte Mikrosegmentierung (29 %) und der Zugriff nach dem Prinzip der geringsten Privilegien (23 %), sind andere Komponenten, die zeigen, wie einzelne Tools und Richtlinien außerhalb einer umfassenden Zero-Trust-Strategie implementiert werden können.

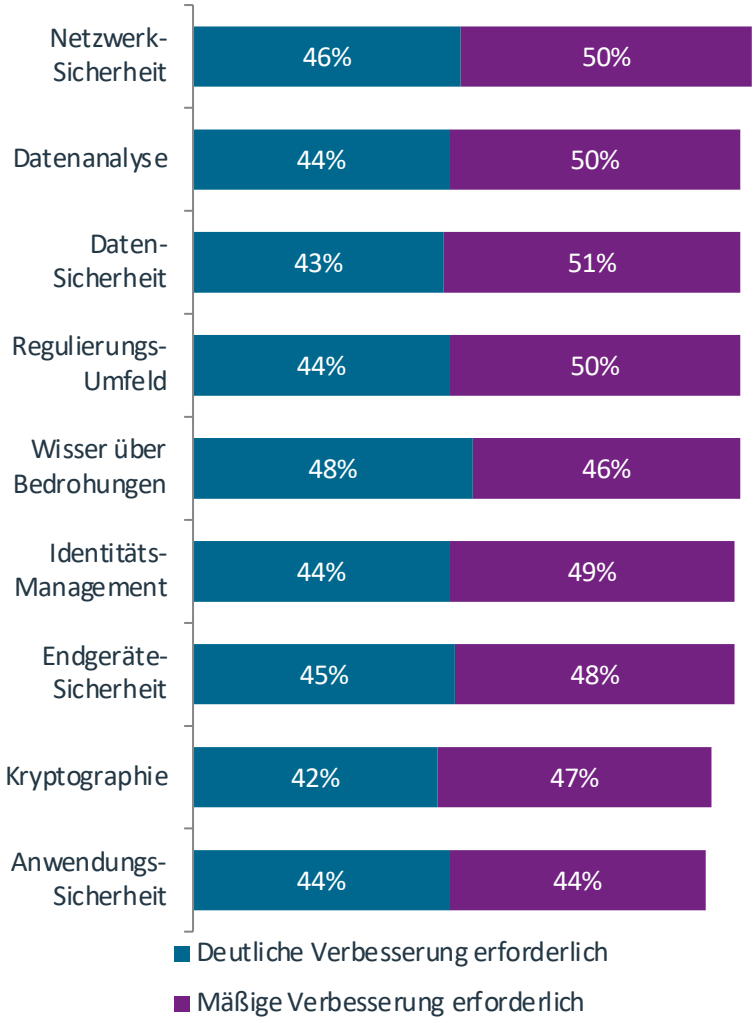
Die wichtigste Erkenntnis ist, dass Zero-Trust eine Philosophie rund um Cybersicherheit ist, die Fragen und Entscheidungen prägt. Die beste Methode, Zero-Trust einzuführen, besteht nicht darin, eine Reihe von Kriterien zu definieren, die auf vollständigen Erfolg hinweisen, sondern eine Roadmap zu erstellen, die die besten Schritte auf der Grundlage des Status des Unternehmens identifiziert. Diese Schritte können eine vollständige Prüfung von Daten und Arbeitsabläufen, die Implementierung spezifischer Produkte wie Identity- und Access-Management-Software (IAM-Software) oder die Gestaltung eines nachhaltigen Schulungsprogramms für die Belegschaft umfassen. Jeder Schritt sollte sich mit einem bestimmten Problem befassen und messbare Ergebnisse haben.

EINBINDUNG VON MENSCHEN UND PRODUKTE IN DIE STRATEGIE

Wenn Unternehmen versuchen, die Grundursache ihrer Sicherheitsmängel zu beheben, werden sie entdecken, dass das Problem mehrere Ebenen hat. Selbstverständlich gibt es die technische Ebene, die seit Jahren im Mittelpunkt steht und weiterhin ein wesentlicher Bestandteil einer Cybersicherheitslösung ist. Es gibt auch die Belegschaftsebene, und viele Unternehmen haben sich der Aufklärung über Cybersicherheit verschrieben, um in diesem Bereich Verbesserungen zu erzielen. Andere Ebenen, die sich mit betrieblichen Abläufen und der Bewertung von Unternehmen befassen, haben in den letzten Jahren jedoch wohl weniger Aufmerksamkeit erhalten.

Da sich Unternehmen darauf konzentrieren, die Cybersicherheitskette so zu kultivieren, dass sie alle Ebenen des Unternehmens umfasst, werden technische Spezialisten immer eine entscheidende Komponente sein. Nach einer gründlichen Bewertung des Kompetenzdefizits ist die Verbesserung der Kompetenz die nächste Herausforderung. Netzwerksicherheit mag wie ein Bereich mit tiefgreifendem Fachwissen erscheinen, da die Aufgabe seit langem erfüllt wird. Aber Tatsache ist, dass Veränderungen in der IT-Landschaft eine ständige Verbesserung erfordern. Andere Bereiche, wie Kenntnis der Bedrohungen, Datenanalyse und Identitätsmanagement, sind offensichtlichere Kandidaten für die Verbesserung der Kompetenz, da sie neuere Trends in der Cybersicherheit repräsentieren.

Anforderungen an Cybersicherheitskompetenzen



Die Cybersicherheits-Produktliste beginnt mit Teilen, die es schon lange gibt. Firewalls, Antivirenprogramme und Anti-Malware waren die Hauptkomponenten des sicheren Umfelds, und sie eignen sich nach wie vor für diesen Zweck, selbst wenn das sichere Umfeld an Bedeutung verloren hat. Diese Tools sind allgegenwärtig, wenngleich viele Endbenutzer (und möglicherweise sogar IT-Mitarbeiter) sie möglicherweise nicht als Teil des Produktsets erachten, da sie so geläufig sind.

Netzwerküberwachung ist ein weiteres Tool, das es schon lange gibt und das sich weiterentwickelt, um zeitgemäß zu sein. Tools wie SolarWinds Network Performance Monitor, Datadog Network Monitoring und Auvik bieten umfangreiche Möglichkeiten zur Beobachtung und Analyse einer gesamten Netzwerkarchitektur. Zu den neuesten Funktionen bei Netzwerkmonitoren gehören die Transparenz von Cloud-Komponenten des Netzwerks und Analysetools, um den Datenfluss besser zu verstehen.

Da SaaS-Monitoring- und -Management-Tools die Bedeutung von Cloud-Systemen herausstellen, gewinnen sie schnell an Bedeutung. Die Beschleunigung der Cloud-Einführung war eine der größten Veränderungen in IT-Vorgängen während der Pandemie, und Unternehmen reagieren jetzt auf die Auswirkungen dieser Sekundäreffekte. Neben Cybersicherheitsproblemen werden Cloud-Systeme von einer einzigartigen Reihe von Bedenken in Bezug auf Nutzung und Kosten begleitet, und neue Management-Software ist erforderlich, um die Cloud-Architektur ordnungsgemäß zu verwalten, zu inszenieren und zu sichern.

Am anderen Ende des Spektrums gibt es Tools, die noch immer selten angewendet werden, aber als anstehende Ergänzungen stark in Betracht gezogen werden sollten. Wenngleich SaaS die beliebteste Form der Cloud-Einführung ist, ist IaaS ebenfalls weit verbreitet und kann für eine ordnungsgemäße Überwachung und Verwaltung ausschlaggebender sein. Umfassende Netzwerk-Überwachungstools sind entscheidend, um einen Überblick über das große Ganze zu erhalten, aber Paket-Sniffer und LAN-Analysatoren sind anvisierte Produkte, die schwer zu findende Probleme aufspüren können.

Mit so vielen Tools im Arsenal und so vielen Beschränkungen beim Cybersicherheitspersonal ist der offensichtlich nächste Schritt die Automatisierung. Die Automatisierung durchdringt die Komplexität der Einführung mehrerer Produkte, aber sie beseitigt nicht unbedingt den Bedarf an Cybersicherheitsspezialisten. Neues Fachwissen ist erforderlich, um die Automatisierung ordnungsgemäß zu implementieren und bei Bedarf laufende Anpassungen durchzuführen.

Die Automatisierung löst das Ressourcenproblem zwar nicht vollständig, sie macht die Situation aber überschaubarer. Die Integration von Cybersicherheit in den Geschäftsbetrieb macht Cybersicherheit noch ausschlaggebender als je zuvor, und die Umsetzung einer Zero-Trust-Philosophie führt zu einer Reihe neuer Verfahren. Eine zweckbestimmte Unternehmensstruktur und das richtige Tool-Set sind die ersten Schritte bei der Bewältigung zusätzlicher Komplexität. Durch einen ausgewogenen Ansatz für die Automatisierung können Unternehmen ihre zugrundeliegenden Schwierigkeiten vollständig angehen und sich in Richtung einer gesunden Entwicklung der Cybersicherheit bewegen.