Acht ausschlaggebende Elemente der Cybersicherheit

Veröffentlicht am 15. April 2024

Mobeen Tahir
Director, Macroeconomics and Thematic Research

Die wichtigsten Erkenntnisse

- Mit der Einführung digitaler Tools in Unternehmen nehmen die Risiken für die Cybersicherheit zu.
- Von der Sicherung von Daten bis hin zu Geräten und der Schulung des Personals – Cybersicherheit hat viele Facetten.
- Unternehmen, die einen breiten Fokus auf mehrere Bereiche der Cybersicherheit legen, haben potenziell bessere Chancen, in einer sich schnell entwickelnden Branche zu bestehen.

Am 19. Februar berichtete die Financial Times,[1] dass nordkoreanische Cyberkriminelle auf künstliche Intelligenz (KI) zurückgreifen, um Gelder und Spitzentechnologien von Opfern in aller Welt zu stehlen. In dem Bericht wurde beschrieben, wie Hacker gezielt globale Verteidigungs-, Cybersicherheits- und Kryptounternehmen angegriffen haben, indem sie Menschen auf beliebten Plattformen wie LinkedIn hinters Licht geführt haben. Er wies außerdem darauf hin, dass der ChatGPT-Entwickler OpenAI und dessen Investor Microsoft ebenfalls bestätigt haben, dass Kriminelle ihre KI-Dienste für böswillige Cyberaktivitäten nutzen.

Generative KI-Tools haben die Hürde für Menschen gesenkt, die mit relativ einfachen Fähigkeiten technisch anspruchsvollere Dinge erreichen wollen. Große Sprachmodelle ermöglichen es Benutzern, mit dem Computer in einer Sprache wie Englisch zu kommunizieren und das Modell ihre Befehle übersetzen zu lassen, um Programme zu schreiben. Leider kann die Technologie auch dazu führen, dass Kriminelle leichter illegale Aktionen durchführen können. Aus diesem Grund muss die Cybersicherheit intelligenter werden und alle potenziellen Schwachstellen schließen, bevor Kriminelle sie ausnutzen.

WisdomTree hat gemeinsam mit der Venture-Gruppe Team8 acht verschiedene Bereiche der Cybersicherheit identifiziert, die in einer Welt mit ständig wachsenden Risiken von entscheidender Bedeutung sind.

Damit Cybersicherheit zuverlässig ist, muss sie ganzheitlich sein

Quelle: WisdomTree, Team8, 2024.

Datensicherheit

Schätzungen zufolge produziert die Welt jeden Tag 328 Millionen Terabyte an Daten. Ein Terabyte entspricht 1000 Gigabyte. Mit anderen Worten: Die Welt produziert eine Menge Daten. Außerdem pro-

duziert die Welt Daten schneller als je zuvor. Es wird außerdem angenommen, dass 90% der weltweiten Daten allein in den letzten zwei Jahren erzeugt wurden[2].

IBM gibt an, dass die durchschnittlichen Kosten für Datenschutzverletzungen im Jahr 2023 bei 4,45 Mio. USD liegen, was einem Anstieg von 15 % innerhalb von drei Jahren entspricht[3]. Da die Welt mehr Daten produziert als je zuvor, ist der Schutz dieser Daten von größter Bedeutung. Das ist es, was die Datensicherheit erreichen soll.

Cloud-Sicherheit

All diese Daten, die produziert werden, bedeuten mehr Speicherplatz in der Cloud. Einem Bericht zufolge[4] werden etwa 60 % aller Unternehmensdaten in der Cloud gespeichert, im Jahr 2015 waren es nur 30 %. Darüber hinaus verwenden 89 % der Unternehmen einen Multi-Cloud-Ansatz, ein Begriff, der sich auf Unternehmen bezieht, die mindestens zwei Cloud-basierte Anwendungen nutzen.

Und leider sind sich Kriminelle dessen voll bewusst. Im Jahr 2023 gab es einen Anstieg von 110 % bei den Fällen, in denen die Cloud eine wichtige Rolle spielte[5]. Das bedeutet, dass Cyber-Angreifer zunehmend versuchen, ihre Ziele über Cloud-basierte Anwendungen anzugreifen. Die Absicherung der Cloud ist daher ein wichtiges Thema der Cybersicherheit.

Shift-Left

Die Absicherung der Cloud oder jeder anderen Anwendung darf nicht auf die lange Bank geschoben werden. Shift-Left bezieht sich auf die Idee, die Cybersicherheit bereits bei der Entwicklung der Software zu integrieren. Das Gegenteil davon wäre, die Cybersicherheit hintanzustellen und sich auf generische Lösungen von Drittanbietern zu verlassen.

Die Berücksichtigung Cybersicherheit in einer frühen Projektphase ermöglicht es Entwicklern, Schwachstellen in der Software kritisch zu bewerten, um sicherzustellen, dass alle erforderlichen Schutzmaßnahmen bereits bei der Erstellung der Software vorhanden sind. Dies kann die Kosten senken und die Bereitstellung beschleunigen, da es wahrscheinlich weniger Probleme geben wird, sobald die Software bei den Anwendern eingeführt ist.

Intelligente Sicherheit

Die generative KI hat die Hürde, ein krimineller Akteur zu werden, gesenkt. Es ist jetzt einfacher, bösartigen Code zu erstellen, wie z. B. bei einem polymorphen Angriff, bei dem der Cyberangriff Code, Inhalt und Struktur verändert, um von Sicherheitssystemen nicht entdeckt zu werden. Ein derartiger Code funktioniert noch besser, wenn er von den Sicherheitsvorkehrungen eines Unternehmens blockiert wurde.

Die Abwehr solcher Bedrohungen erfordert Automatisierung. Zu intelligenter Sicherheit gehören Automatisierungstools, die Netzwerke auf potenzielle Bedrohungen überwachen können. Hier spielen KI-Tools, die lernen, sich anpassen und weiterentwickeln, eine entscheidende Rolle für die Gewährleistung der Sicherheit.

Security of Things

Das sogenannte Internet of Things (IoT) bezieht sich auf Geräte, die mit dem Internet verbunden sind. Laptops und Mobiltelefone sind offensichtliche Beispiele, aber jetzt gehören auch Autos, Uhren, digitale Assistenten, Fernseher, Geschirrspüler und dergleichen zunehmend zur IoT-Welt. Schätzungen zufolge gibt es derzeit 17 Milliarden IoT-Geräte auf der Welt, und diese Zahl könnte sich bis 2030 verdoppeln[6].

Es liegt auf der Hand, dass unsere Geräte geschützt werden müssen, da sie Angreifern Angriffspunkte für den Zugriff auf unsere Netzwerke und Daten bieten. Bei der Security of Things geht es also darum, diese wachsende Zahl von vernetzten Geräten vor potenziellen Bedrohungen zu schützen.

Perimeterlose Welt

Die so genannte Angriffsfläche hat sich vergrößert, da Organisationen seit der COVID-19-Pandemie eine größere Anzahl von Beschäftigten haben, die remote arbeiten. Diese Angriffsfläche bezieht sich auf die Summe der Schwachstellen, die Hacker ausnutzen können, um auf das Netzwerk eines Unternehmens oder sensible Daten zuzugreifen. Im Vergleich zu früher, als Beschäftigte innerhalb eines bestimmten Perimeters aufzufinden waren, haben Angreifer heute mehr potenzielle Einstiegspunkte.

In einer perimeterlosen Welt brauchen Unternehmen ausgefeiltere Werkzeuge, um sich zu schützen. Dazu gehören die Zwei-Faktor-Authentifizierung und die Biometrie für Anwender, die sich bei ihrem Firmennetzwerk und ihren Anwendungen anmelden.

Resilienz & Wiederherstellung

Im Mai 2017 kostete der WannaCry-Ransomware-Angriff den britischen National Health Service 92 Millionen Brtische Pfund durch den Ausfall von Dienstleistungen und IT-Kosten. Noch wichtiger ist, dass 19.000 Termine abgesagt wurden, da mehr als 80 Krankenhäuser und 8 % der Hausarztpraxen betroffen waren[7].

Laut Team8 kann sich Cybersicherheit nicht auf „Identifizieren, Schützen, Erkennen und Reagieren“ beschränken, sondern muss auch die Fähigkeit zur schnellen Wiederherstellung nach einer Beeinträchtigung, Störung oder Verweigerung des Zugriffs auf das Netzwerk oder die Daten eines Unternehmens umfassen. Die Kosten, die entstehen, wenn man nicht in der Lage ist, dies zu tun, können katastrophal sein.

Ein Unternehmen mag über die leistungsfähigsten Cybersicherheits-Tools verfügen, um sich zu schützen. Aber wenn die Angestellten nicht geschult und ausgerüstet sind, um mit Risiken umzugehen, können die Schutzvorrichtungen wie ein Kartenhaus in sich zusammenfallen. Layer 8 ist demnach der menschliche Faktor.

Laut CrowdStrike waren 75 % der Angriffe im Jahr 2023 frei von Malware, gegenüber 40 % im Jahr 2019. Das bedeutet, dass die Angreifer weniger auf Malware-Angriffe über Phishing-E-Mails setzen, sondern auf ausgefeiltere Methoden wie Social Engineering, die darauf abzielen, Menschen zu täuschen. Die Fähigkeit

der Einzelnen, Cybersecurity-Risiken besser zu managen, kann daher die Grundlage für alle anderen Maßnahmen sein.

Cybersecurity ist nicht optional. Ihre Bedeutung wird nur allzu deutlich, wenn ein erfolgreicher Angriff stattfindet. Aber dann kann es bereits zu spät sein, um größere Schäden zu verhindern. Ein Rahmen für die Cybersicherheit, der einen ganzheitlichen Ansatz für diese acht wesentlichen Elemente verfolgt, bietet Unternehmen die besten Chancen, unerwünschte Ergebnisse zu vermeiden.

[1] https://www.ft.com/content/728611e8-dce2-449d-bb65-cff11ac2a5bb
[2] Quelle: explodingtopics.com (Stand: Dezember 2023), das Statista als Informationsquelle angibt. Explodingtopics.com/blog/data-generated-per-day
[3] IBM – Cost of a Data Breach Report 2023
[4] Quelle: explodingtopics.com (Stand: November 2023), das Thales Group als Informationsquelle angibt. Explodingtopics.com/blog/corporate-cloud-data
[5] CrowdStrike 2024 Global Threat Report.
[6] Quelle: explodingtopics.com (Stand: Februar 2024), das Transforma Insights als Informationsquelle angibt. Explodingtopics.com/blog/number-of-iot-devices
[7] National Health Executive, Oktober 2018.

Important Risks Related to this Article

Wichtige Informationen

Im Europäischen Wirtschaffsraum („EWR“) herausgegebene Marketingkommunikation: Dieses Dokument wurde von WisdomTree Ireland Limited, einer von der Central Bank of Ireland zugelassenen und regulierten Gesellschaff, herausgegeben und genehmigt.

In Ländern außerhalb des EWR herausgegebene Marketingkommunikation: Dieses Dokument wurde von WisdomTree UK Limited, einer von der United Kingdom Financial Conduct Authority zugelassenen und regulierten Gesellschaff, herausgegeben und genehmigt.

WisdomTree Ireland Limited und WisdomTree UK Limited werden jeweils als „WisdomTree“ bezeichnet. Unsere Richtlinie über Interessenkonflikte und unser Verzeichnis sind auf Anfrage erhältlich.

Nur für professionelle Kunden. Wertsteigerungen in der Vergangenheit lassen keinen Schluss auf zukünffige Ergebnisse zu. Jegliche in diesem Dokument enthaltene historische Wertentwicklung kann u. U. auf Backtesting beruhen. Backtesting ist der Prozess, bei dem eine Anlagestrategie evaluiert wird, indem sie auf historische Daten angewandt wird, um zu simulieren, was die Wertentwicklung solch einer Strategie in der Vergangenheit gewesen wäre. Durch Backtesting erzielte Wertsteigerungen sind rein hypothetisch und werden in diesem Dokument einzig und allein zu Informationszwecken aufgeführt. Daten, die durch Backtesting gesammelt wurden, stellen keine tatsächlichen Wertsteigerungen dar und dürfen nicht als Indikator für tatsächliche oder zukünffige Wertsteigerungen angesehen werden. Der Wert jeder Anlage kann durch Wechselkursbewegungen beeinflusst werden. Anlageentscheidungen sollten auf den Angaben im entsprechenden Prospekt sowie auf unabhängiger Anlage-, Steuer- und Rechtsberatung basieren. Diese Produkte sind gegebenenfalls nicht in Ihrem Markt verfügbar oder für Sie geeignet. Der Inhalt dieses Dokuments stellt weder eine Anlageberatung noch ein Angebot zum Verkauf bzw. eine Aufforderung oder ein Angebot zum Kauf eines Produktes oder zum Tätigen einer Anlage dar.

Eine Anlage in börsengehandelte Produkte („ETPs“) ist abhängig von der Wertentwicklung des Basisindexes, abzüglich Kosten, aber es wird nicht erwartet, dass ihre Wertentwicklung genau mit der des Indexes übereinstimmt. ETPs unterliegen mehreren Risiken, darunter allgemeine Marktrisiken im Zusammenhang mit dem jeweiligen Basisindex, Kreditrisiken des Anbieters von Index-Swaps, die im ETP genutzt werden, Wechselkursrisiken, Zinsrisiken, Inflationsrisiken, Liquiditätsrisiken sowie rechtliche und regulatorische Risiken.

Bei den in diesem Dokument enthaltenen Informationen handelt es sich nicht um Werbung bzw. eine Maßnahme zum öffentlichen Angebot der Anteile in den USA oder einer zugehörigen Provinz bzw. einem zugehörigen Territorium der USA, wo weder die Emittenten noch deren Produkte zum Vertrieb zugelassen oder registriert sind und wo die Prospekte der Emittenten nicht bei einer Wertpapieraufsichtsbehörde oder sonstigen Aufsichtsbehörde eingereicht wurden, und dürfen unter keinen Umständen als solche verstanden werden. Weder dieses Dokument noch Informationen in diesem Dokument sollten in die USA mitgenommen, (direkt oder indirekt) übermittelt oder verteilt werden. Weder die Emittenten noch etwaige

von ihnen ausgegebenen Wertpapiere wurden oder werden gemäß dem United States Securities Act von 1933 oder dem Investment Company Act von 1940 registriert oder qualifizieren sich unter jeglichen anwendbaren bundesstaatlichen Wertpapiergesetzen.

Dieses Dokument kann unabhängige Marktkommentare enthalten, die von WisdomTree auf der Grundlage öffentlich zugänglicher Informationen erstellt wurden. Obwohl WisdomTree bestrebt ist, die Richtigkeit des Inhalts dieses Dokuments sicherzustellen, übernimmt WisdomTree keine Gewährleistung oder Garantie für seine Richtigkeit oder Genauigkeit. Die Drittanbieter, deren Dienste in Anspruch genommen werden, um die in diesem Dokument enthaltenen Informationen zu beziehen, übernehmen keine Gewährleistung oder Garantie jeglicher Art bezüglich dieser Daten. Dort, wo WisdomTree seine eigenen Ansichten in Bezug auf Produkte oder Marktaktivitäten äußert, können sich diese Auffassungen ändern. Weder WisdomTree, noch eines seiner verbundenen Unternehmen oder einer seiner jeweiligen leitenden Angestellten, Verwaltungsratsmitglieder, Partner oder Mitarbeiter übernimmt irgendeine Haffung für direkte Schäden oder Folgeschäden, die durch die Verwendung dieses Dokuments oder seines Inhalts entstehen.

Dieses Dokument kann zukunffsorientierte Aussagen enthalten, einschließlich Aussagen hinsichtlich unserer Einschätzung oder aktuellen Erwartungen im Hinblick auf die Wertentwicklung bestimmter Anlageklassen und/oder Sektoren. Zukunffsorientierte Aussagen unterliegen gewissen Risiken, Unsicherheiten und Annahmen. Es gibt keine Sicherheit, dass

diese Aussagen zutreffen, und die tatsächlichen Ergebnisse können von den erwarteten Ergebnissen abweichen. WisdomTree empfiehlt Ihnen deutlich, sich nicht in unangemessener Weise auf diese zukunffsgerichteten Aussagen zu verlassen.

WisdomTree Issuer ICAV

Die in diesem Dokument erörterten Produkte werden von WisdomTree Issuer ICAV („WT Issuer“) begeben. WT Issuer ist eine als Umbrella-Fonds strukturierte Anlagegesellschaff mit variablem Kapital und Haffungstrennung zwischen den Fonds, die nach irischem Gesetz als Irish Collective Asset-management Vehicle errichtet und von der Zentralbank von Irland („CBI“) zugelassen wurde. Die WT-Emittentin ist als Organismus für gemeinsame Anlagen in Wertpapieren („OGAW“) nach irischem Recht strukturiert und gibt eine separate Anteilsklasse („Anteile“) aus, die jeden Fonds repräsentiert. Anleger sollten den Verkaufsprospekt der WT-Emittentin („ WT-Prospekt“) vor einer Investition lesen und im Abschnitt des WT-Prospekts mit dem Titel„ Risikofaktoren“ weitere Einzelheiten über die mit einer Anlage verbundenen Risiken in entsprechende Anteile erfahren.

Für Anleger in der Schweiz – Qualifizierte Anleger

Dieses Dokument dient als Werbung für die hier genannten Finanzprodukte.

Der Verkaufsprospekt und die wesentlichen Anlegerinformationen (KIID) sind auf der Website von WisdomTree verfügbar: **https:** //www.wisdomtree.eu/de-ch/resource-library/prospectus-and-regulatory-reports

Einige der Teilfonds, auf die in diesem Dokument verwiesen wird, wurden möglicherweise nicht bei der Eidgenössischen Finanzmarktaufsicht („FINMA“) registriert. In der Schweiz werden solche Teilfonds, die nicht bei der FINMA registriert sind, ausschließlich an qualifizierte Anleger im Sinne des Schweizer Bundesgesetzes über die kollektiven Kapitalanlagen oder seiner Durchführungsverordnung (jeweils in der jeweils gültigen Fassung) vertrieben. Die Vertretung und Zahlstelle der Teilfonds in der Schweiz ist Société Générale Paris, Niederlassung Zürich, Talacker 50, Postfach 5070, 8021 Zürich, Schweiz. Der Prospekt, die wesentlichen Anlegerinformationen, die Satzung sowie die Jahres- und Halbjahresberichte der Teilfonds sind kostenlos bei der Vertretung und Zahlstelle erhältlich. Hinsichtlich des Vertriebs in der Schweiz befinden sich der Erfüllungsort und Gerichtsstand am Sitz der Vertretung und Zahlstelle.

Für französische Anleger

Die in diesem Dokument enthaltenen Informationen richten sich ausschließlich an professionelle Anleger (wie im Rahmen der MiFID definiert), die auf eigene Rechnung investieren, und dieses Material darf in keiner Weise öffentlich verteilt werden. Die Verteilung des Prospekts und das Angebot, der Verkauf und die Lieferung von Anteilen in anderen Ländern können gesetzlichen Beschränkungen unterliegen. Der Emittent ist ein OGAW, der der irischen Gesetzgebung unterliegt, und von der Finanzaufsichtsbehörde als OGAW, der den europäischen Verordnungen entspricht, zugelassen. Dennoch muss er möglicherweise nicht denselben Regeln entsprechen, die für ein ähnliches Produkt gelten, das in Frankreich zugelassen wurde. Der Fonds wurde in Frankreich von der Finanzaufsichtsbehörde (Autorité des Marchés Financiers) für den Vertrieb registriert und darf an Anleger in Frankreich vertrieben werden. Exemplare aller Dokumente (d. h. des Prospekts, des Dokuments mit den wesentlichen Informationen für den Anleger, aller zugehörigen Ergänzungen oder Nachträge, der neuesten Jahresberichte und der Gründungsurkunde und Satzung) sind in Frankreich kostenlos bei der französischen Zentralisierungsstelle Societe Generale unter der Adresse 29, boulevard Haussmann – 75009 Paris, Frankreich, erhältlich. Alle Zeichnungen von Anteilen des Fonds erfolgen auf der Grundlage der Bedingungen des Prospekts und aller zugehörigen Ergänzungen oder Nachträge.