valantic

SCHUTZ VON GESCHÄFTSGEHEIMNISSEN

Sensible Daten im Visier: Prävention und Schutz in der digitalen Ära

Inhalt

Liebe Leserin, lieber Leser,

im digitalen Zeitalter stehen Unternehmen vor der ständigen Herausforderung, ihre sensiblen Informationen und Betriebsgeheimnisse wirksam gegen die wachsende Zahl von Cyberangriffen zu schützen. Eine aktuelle Umfrage des Digitalverbandes Bitkom zeigt, dass zwei Drittel der deutschen Unternehmen ihre Existenz durch solche Bedrohungen gefährdet sehen. Besonders Ransomware-Angriffe und der Diebstahl vertraulicher Informationen stellen aktuelle und ernstzunehmende Risiken dar.

Dieses Whitepaper bietet Ihnen einen umfassenden Überblick über die neuesten Technologien und Strategien zur Abwehr von Cyberbedrohungen. Von Authentifizierungsmethoden und -verfahren, über Data Loss Prevention bis hin zur Netzwerküberwachung – wir beleuchten die Maßnahmen, die Ihnen dabei helfen können, Ihre Unternehmenswerte zu schützen.

Wir möchten Ihnen praktikable und wirkungsvolle Ansätze an die Hand geben, um Ihre Betriebsgeheimnisse in einer unsicheren und sich schnell wandelnden digitalen Landschaft zu sichern. Nutzen Sie dieses Whitepaper, um sich über die neuesten Entwicklungen zu informieren und Ihre Sicherheitsstrategie entsprechend anzupassen.

Wir wünschen Ihnen eine aufschlussreiche Lektüre.

Mit besten Grüßen, Ihre Autoren,
Dr. Werner Gutau und Thomas Lang

Dr. Werner Gutau

consulting@gutau.de

Seit mehr als 25 Jahren hat Werner Gutau als CISO und als Bereichs-CSO Sicherheitsanforderungen mit betrieblichen Belangen in Einklang gebracht. Sein Schwerpunkt lag dabei in der High-Tech-Industrie, wo hohe Sicherheitsanforderungen, IP-Schutz und komplexe, globale Lieferketten zum Tagesgeschäft gehören. Mit Risiko-basierten Ansätzen und Pragmatismus stellt er sowohl Kunden als auch Regelsetzer und Zertifizierer zufrieden. Daneben hat er seine Erfahrung erfolgreich in die Gremienarbeit eingebracht und dabei Sicherheitsstandards geprägt. Seit dem Ausscheiden aus dem „regulären" Berufsleben gibt er seine Erfahrung als Berater weiter.

Thomas Lang

thomas.lang@mc.valantic com

Nach über 20 Jahren als Berater und Unternehmer ist für Thomas Lang das schnelle Einarbeiten auch in kritische Situationen in „Fleisch und Blut" übergegangen. Er bewahrt in jeder Lage Ruhe, kann Wichtiges von Unwichtigem trennen und gibt Dingen Struktur. Das hilft ihm, um in schwierigen Situationen den Überblick zu bewahren. Zu seinen Beratungsschwerpunkten gehören neben den Themen Cybersicherheit & Compliance unter anderem die Themen IT-Strategie, Projekt-Governance und -Controlling, Krisenmanagement sowie IT-Infrastruktur & Betrieb.

Betriebsgeheimnisse sicher vor Cyberangriffen schützen

Zwei Drittel aller deutschen Unternehmen sehen sich durch Cyberattacken in ihrer Existenz bedroht, hat eine Umfrage 2024 des Digitalverbandes Bitkom unter mehr als 1.000 Führungskräften ergeben. Das ist ein beunruhigend hoher Wert. 80 Prozent der Umfrageteilnehmer berichten, dass sich die Anzahl der Cyberattacken auf ihr Unternehmen in den vergangenen zwölf Monaten erhöht habe (Bitkom Research, 2024).

Ransomware 2024/25: Verschlüsselung plus Datendiebstahl

Gefährliche Ransomware-Attacken, die Systeme und Daten verschlüsseln und erst nach Zahlung eines Lösegeldes wieder freigeben, haben laut Bitkom (2024) ein neues Allzeithoch erreicht. Bei 31 Prozent der Umfrageteilnehmer hat Ransomware in den vergangenen zwölf Monaten teils enorme Schäden verursacht. Ransomware bleibt auch in 2025 eine der größten Bedrohungen und wird häufig mit dem Diebstahl von Geschäftsgeheimnissen kombiniert.

Cyberkriminelle gehen dabei nach einem altbewährten, aber immer wieder erfolgreichen Angriffsmuster vor. **Verführerische Phishing-Mails** sind das Einfallstor für die meisten Ransomware-Attacken, wobei **KI-generierte E-Mails und Deepfake-Imitationen** immer überzeugender wirken. Mitarbeitenden-Schulungen und Phishing-Erkennungssysteme können zwar helfen, Ransomware-Angriffe zu unterbinden und den Cyberkriminellen einen Schritt voraus zu sein. Diese nächste Generation von Phishing-Angriffen wird sich jedoch die Fähigkeit der KI zunutze machen, aus Echtzeitdaten zu lernen und sich an fortschrittliche Sicherheitsmaßnahmen anzupassen.

Folgerichtig wird selbst die Hype-Technologie **Künstliche Intelligenz** von 83 Prozent der befragten Führungskräfte eher kritisch als Risikofaktor eingestuft, weil sie die Bedrohungslage verschärft (Bitkom Research, 2024). Generative KI wird Operationen in viel größerem Maßstab ermöglichen. Cyberkriminelle können beispielsweise KI einsetzen, um Tausende gezielter Phishing-Angriffe gleichzeitig zu starten und jeden einzelnen auf maximale Wirkung anzupassen.

Das lässt nur einen Schluss zu: **Kein Unternehmen vom Mittelständler bis zum Großkonzern kann sich sicher fühlen.** Die Welt wird tendenziell, auch durch KI, zu einem sehr unsicheren Ort. Was können Unternehmen tun, um sich gegen eine wachsende Bedrohungslage zu schützen?

Betriebsgeheimnisse sind Ziel #1

Besonders häufig haben es die Angreifer nicht nur auf die Verschlüsselung von Daten, sondern vor allem auf den Diebstahl von Geschäftsgeheimnissen wie Strategiepapieren, Finanzdaten, Blaupausen zukünftiger Produkte oder Kundendaten abgesehen, die dann im Darknet an den Meistbietenden versteigert und zu Geld gemacht werden. Die Schäden, die betroffenen Unternehmen drohen, sind kaum realistisch abzuschätzen und reichen von Umsatzausfällen in Millionenhöhe bis hin zur Bedrohung der gesamten Existenz. Oft unbemerkt: Angreifer sind durchschnittlich über 200 Tage im Unternehmensnetz und lesen mit, bevor sie überhaupt entdeckt werden.

Beliebt ist zum Beispiel der Diebstahl von Zugangsdaten und Passwörtern, die dazu dienen, größere Angriffe in Zukunft vorzubereiten. Accounts von Führungskräften mit sehr weitreichenden Zugriffsrechten stehen dabei besonders im Visier der Angreifer.

83%

der befragten Führungskräfte sagen, dass Künstliche Intelligenz die Bedrohungslage für die Wirtschaft verschärft (Bitkom Research, 2024).

Welche betrieblichen Informationen sind überhaupt schützenswert?

Kein Unternehmen will, dass seine Betriebsgeheimnisse in fremde Hände fallen. Der erste Schritt besteht deshalb darin, sich einen Überblick zu verschaffen und sensible Geschäftsgeheimnisse sowie die Prozesse, in denen sie benötigt werden, zu identifizieren. Eine Schutzbedarfsanalyse (Business Impact Analyse) hilft, den benötigten Schutzgrad zu bestimmen sowie Budgets und Maßnahmen zu priorisieren. Zur Identifikation schützenswerten Informationen gehören unter anderem Strategiepapiere, Know-how, Kalkulationsgrundlagen und Zugangsdaten zu Konten und Finanzsystemen.

Alles, was sie selbst gerne über ihre Wettbewerber und Kunden wissen möchten, ist für Dritte auch über ihr Unternehmen interessant. Besonders vertrauliche und streng vertrauliche Informationen, deren Veröffentlichung die Erreichung der Geschäftsziele gefährdet, bedürfen eines besonderen Schutzes.

Betriebsgeheimnisse laut Gesetz

Hinzu kommt ein juristischer Aspekt: Ein Geschäftsgeheimnis ist nach §2 Abs. 1 des GeschGehG eine Information,

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von **wirtschaftlichem Wert** ist und

b) die Gegenstand von den Umständen nach **angemessenen Geheimhaltungsmaßnahmen** durch ihren rechtmäßigen Inhaber ist und

c) bei der ein **berechtigtes Interesse** an der Geheimhaltung besteht.

Informationen und Daten, die nicht angemessen geschützt sind, sind also nach deutschem Recht keine Betriebsgeheimnisse und ein eventueller Schaden kann nicht geltend gemacht werden.

Entsprechende Gesetze gibt es in den meisten westlichen Ländern, aber auch z.B. in China.

Die wichtigsten Sicherheitsmaßnahmen

Gerne vergessen werden **physikalische Diebstähle** in den Unternehmensgebäuden vor Ort. Zu den physischen Schutzmaßnahmen zählen daher unter anderem auch Zutrittskontrollen am Gebäude, die Aufbewahrung kritischer Dokumente in Safes, ein angemessenes Schlüsselmanagement und die vollständige Vernichtung papierner Dokumente nach Ablauf der Aufbewahrungsfrist durch einen Shredder.

Dagegen werden digitale Cyberattacken, zu denen auch die oben erwähnte Ransomware gehört, durch Cybersicherheitsmaßnahmen weitgehend unterbunden. Zu den wichtigsten Maßnahmen zählen:

Abb. 1: Übersicht der Cybersicherheitsmaßnahmen zur Reduzierung der Angreifbarkeit von Unternehmen
Quelle: valantic

Authentifizierungsmethoden und Verfahren

Es gibt verschiedene Verfahren und Faktoren zur-Authentifizierung und Erfüllung der IT-Sicherheitsziele. Diese Verfahren sind in drei Kategorien einteilbar – wissensbasierte, besitzbasierte und biometrische Faktoren. Je nach Anwendungsbereich eignen sich die Verfahren einzeln oder in Kombination.

Unter die wissensbasierten Faktoren fallen zum Beispiel Passwörter, PINs und Passphrasen. Das Passwort ist die am weitesten verbreitete Authentifizierungsmethode und besteht im Idealfall aus einer zufälligen Ziffern-, Buchstaben- und Sonderzeichenfolge. Hingegen besteht die persönliche Identifikationsnummer (PIN) meist aus einer 4- oder 6-stelligen Ziffernfolge, mit der sich der User an seinem Gerät identifiziert.

Besitzbasierte Faktoren stellen u.a. FIDO und OTP Sicherheitstokens sowie Smartphones und klassische Smartcards dar. Sicherheitstokens dienen meist der zusätzlichen Absicherung von Benutzerkonten. Sie fungieren als zweiter Faktor, oftmals in Form eines USB-Sticks, und können einem Benutzer eindeutig zugeordnet und somit personalisiert werden. Sicherheitstokens generieren ein One Time Password (OTP). Das Smartphone dient als gängiges Authentifizierungsmedium.

Die dritte Kategorie der Authentifizierungsmethoden bilden die biometrischen Faktoren. Darunter fallen zum Beispiel Fingerabdruck- und Iris-Scanner sowie die Venen- oder Gesichtserkennung, das Tippverhalten und die Spracherkennung. Davon durchgesetzt haben sich der Fingerabdruck und die Gesichtserkennung.

Multifaktor-Authentifizierung

Als Multi-Faktor-Authentifizierung (MFA) bezeichnet man den Nachweis der Identität eines Nutzers über mehr als einem Faktor (z.B. Passwort + One-Time-Password (OTP) oder Passwort + Fingerabdruck + Sicherheitstoken). Die Multifaktor-Authentifizierung gilt als besonders sicher.

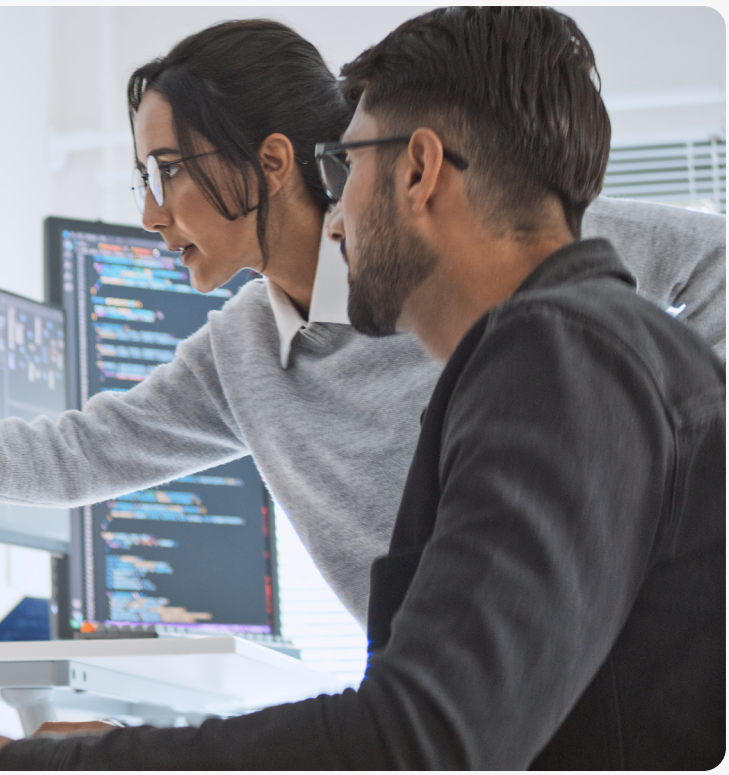
DLP Systeme

Data Loss Prevention (DLP) ist eine strategische Sicherheitsmaßnahme, die sicherstellt, dass sensible oder kritische Informationen nicht außerhalb

des Unternehmensnetzwerks übertragen werden. Der Administrations- und Schulungsaufwand ist jedoch relativ hoch.

Kryptographische Verfahren

Kryptografische Verfahren sind Verschlüsselungsmethoden, die besonders sensible Inhalte schützen. Die Qualität der kryptografischen Verfahren hängt insbesondere vom verwendeten Verschlüsselungsverfahren und der gewählten Schlüssellänge (z.B. 512 Bit) ab. Mit zunehmender Schlüssellänge wächst die Anzahl der Möglichkeiten, die durchgespielt werden müssen, um eine verschlüsselte Nachricht zu entschlüsseln. Je länger also der Schlüssel, desto besser sind die verschlüsselten Informationen geschützt.



Verschlüsselung von Dateien und Ordnern

Die Datei- und Ordner-Verschlüsselung umfasst die Verschlüsselung einzelner Objekte, wie Container, Ordner oder einzelne Dateien. Daher ist diese Art der Verschlüsselung auch als Objektverschlüsselung bekannt. Objektverschlüsselung bietet die Möglichkeit, Dateien und Ordner sicher von einem Ort zu einem anderen zu transportieren und eine Einsichtnahme durch Unbefugte zu verhindern.

Verschlüsselung von E-Mails

Geschäftliche E-Mails enthalten oft wichtige und schützenswerte Informationen. Die Schutzziele können generell durch die Verschlüsselung des Transportwegs oder der E-Mail-Inhalte erreicht werden.

Sicherung des Datenverkehrs durch PKI

Im digitalen Datenverkehr ist es wichtig, dass die Identität der Kommunikationspartner und die Echtheit der übermittelten Inhalte garantiert wird. Der Nachweis digitaler Identitäten bei Personen und Organisationen lässt sich durch den Einsatz von Zertifikaten sicherstellen. Für den Echtheits-Nachweis von übermittelten Dokumenten und Nachrichten sind elektronische Signaturen geeignet. Auch beim verschlüsselten Datentransport kommen zertifikatsbasierte Lösungen zum Einsatz.

All diese Szenarien setzen allerdings eine Komponente voraus: eine Public Key Infrastructure (PKI).

Netzwerküberwachung durch ein Intrusion Detection System

Ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) erkennt und protokolliert Anomalien im Unternehmensnetz. Das Ziel beider Systeme besteht darin, das Eindringen und Verteilen von Schadsoftware möglichst vor dem Schadenseintritt zu erkennen.

Im Gegensatz zum IDS, welches ausschließlich anomales Verhalten anzeigt und Alarme generiert, kann ein IPS auch selbsttätig eingreifen. Damit soll die weitere Ausbreitung von Schadsoftware über das Firmennetz verhindert werden. Dabei ist zu beachten das zum Beispiel bei Industrie- und Produktionsanlagen oder vollautomatisierten Bestell-/Lieferprozessen sowie Meldungs- und Sicherheitsprozessen (u. a. Brandschutz) ein direkter Eingriff durch ein IPS die Verfügbarkeit der Systeme unmittelbar beeinflusst.

Schutz von Webanwendungen

Eine Web Application Firewall (WAF) schützt Webanwendungen wie Homepages, Online-Shops und Homebanking-Portale vor Angriffen. Die WAF untersucht dazu die Kommunikation zwischen Benutzer und Webapplikation auf Anwendungsebene und blockiert potenziell schädlichen Datenverkehr wie SQL Injections oder Cross-Site-Scripting. Für Machine-to-machine-Kommunikation ist auch die Bezeichnung Web Service Firewall (WSF) gebräuchlich.

Angriffserkennung und Auswertung (SIEM)

Für die Auswertung von Anomalien und Erkennung von Angriffen auf die Unternehmensinfrastruktur werden sogenannte Security Information and Event Management Systeme (kurz: SIEM) eingesetzt. Sie ermöglichen ganzheitlich, sicherheitskritische Events der IT-Infrastruktur in Echtzeit zu erkennen und – teilweise automatisiert - geeignete Abwehrmaßnahmen durchzuführen.

SIEM kann gegen die folgenden Bedrohungen unterstützen: Angriffsaktivitäten durch Externe (Hacker-Angriffe), Bedrohungen durch Insider (z.B. unberechtigte Datei-Zugriffe aus anderen Abteilungen, Computersabotage) und Compliance-Verstöße.

Netzwerksegmentierung und -separierung

Die Aufteilung von Netzwerken durch Netzwerksegmentierung und -separierung ist eine effektive Maßnahme, die Weiterverbreitung von Malware zu verhindern. Bei der Netzwerksegmentierung wird ein Netzwerk in mehrere Segmente unterteilt, von denen jedes als eigenes Teilnetzwerk fungiert. Die Kommunikation zwischen diesen Segmenten erfolgt eingeschränkt über definierte Zonengrenzen (Boundary Protections). Dadurch werden Segmente im Netzwerk vor Angriffen aus anderen, bereits betroffenen Segmenten geschützt.

Penetrationtests

Regelmäßige Penetrationstests sind simulierte Angriffe auf ihre Netzwerke, die Lücken und Konfigurationsfehler aufdecken können. bevor ein Schaden entsteht. Das ist oft sinnvoll, bevor neue Anwendungen oder Systeme freigegeben werden.

Darknet Monitoring

Abhanden gekommene geschäftskritische Informationen können schwerwiegende Folgen haben. Wer über den Verlust informiert ist, kann reagieren. Wie in der realen Welt, wo Diebesgut auf dem Schwarzmarkt gehandelt wird, werden im Internet entwendete Unternehmensinformationen wie gestohlene Anmeldeinformationen oder Zahlungsverkehrsinformationen im sogenannten Dark Web gehandelt. Darunter versteht man eine Vielzahl separater, nicht öffentlich zugänglicher Netzwerke (Darknets) innerhalb des Internets.

Tauchen also zum Beispiel Anmeldeinformationen für Unternehmens-Accounts im Darknet auf, lässt das Rückschlüsse auf einen bevorstehenden Angriff auf das kompromittierte Unternehmen zu.

Threat Intelligence

Threat Intelligence (Cyberrisiko-Aufklärung) sammelt, analysiert und priorisiert potenzielle und aktuelle Bedrohungen von IT-Systemen, Netzwerken und Organisationen. Threat Intelligence greift dafür auf interne Daten (z.B. Log-Protokolle) und externe Quellen (z.B. Darknet/Dark Web) zurück. Das Ziel besteht darin, Bedrohungen früher zu erkennen, Reaktionszeiten zu verkürzen und durch vorbeugende Maßnahmen Risiken zu reduzieren.

Supply Chain Security

Grundsätzlich sollten Partner dasselbe Schutzniveau wie der Auftraggeber erreichen. Das ist in Verträgen zu spezifizieren, die Einhaltung muss überprüft werden. Zu bekannten Third-Party-Risk-Management-Diensteistern zählen zum Beispiel Bitsight, Panorays, SecurityScorecard und andere.

Top-Risiko: unüberlegter Einsatz von KI-Tools

Da KI sowohl im privaten als auch im beruflichen Umfeld immer allgegenwärtiger wird, wächst die Gefahr eines unsachgemäßen Einsatzes von KI-Tools. Eines der größten Risiken im Jahr 2025/26 werden Datenschutzverletzungen sein, die dadurch verursacht werden, dass Mitarbeitende unbeabsichtigt sensible Informationen mit KI-Plattformen wie ChatGPT oder Google Gemini teilen. KI-Systeme können riesige Datenmengen verarbeiten und wenn diese Daten in externe KI-Tools eingespeist werden, steigt das Risiko dramatisch.

So könnten Mitarbeitende beispielsweise sensible Finanzdaten in ein KI-Tool eingeben, um einen Bericht oder eine Analyse zu erstellen, ohne sich darüber im Klaren zu sein, dass ihre Daten gespeichert und von fremden, unbefugten Nutzern abgerufen werden könnten.

KI-generierte Malware und Multi-Agenten-Systeme

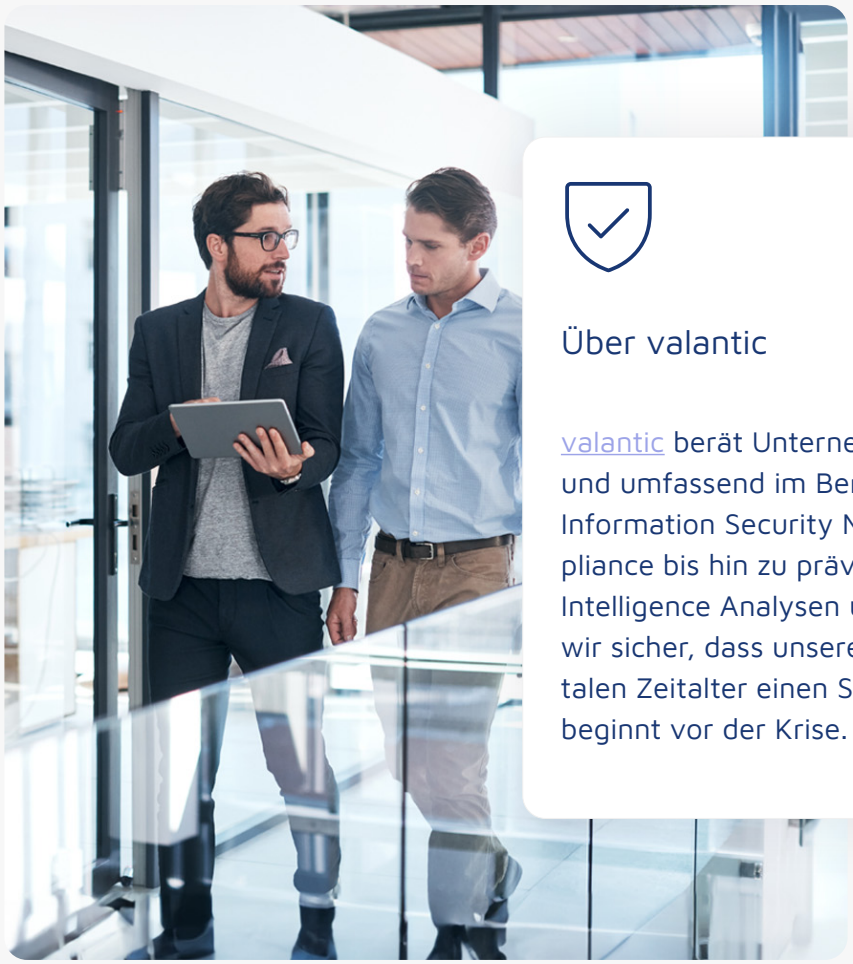
Angreifer werden in zunehmendem Maße fortschrittliche KI-Tools, die über Tools zur Code-Vervollständigung wie GitHub Copilot hinausgehen, zur Code-Generierung nutzen. KI-Plattformen werden in der Lage sein, mit einer einzigen Eingabeaufforderung einen vollständigen Code für Malware zu programmieren.

Dieser Trend fördert die rasche Erstellung ausgeklügelter und hochgradig zielgerichteter Cyberbedrohungen. Die Einstiegshürde für böswillige Akteure sinkt drastisch und die Welt wird zu einem weitaus weniger sicheren Ort. Denn die Tools sind leicht zugänglich, schwer zu entdecken und entwickeln sich schneller weiter, als sich herkömmliche Sicherheitsabwehrsysteme anpassen können.

Es werden Multi-Agenten-KI-Systeme entstehen, bei denen mehrere KI-Modelle zusammenarbeiten und komplexe Probleme lösen. Angreifer werden diese Systeme nutzen, um koordinierte, verteilte Angriffe auszuführen, die schwieriger zu erkennen und abzuwehren sind. Gleichzeitig werden Verteidiger ähnliche Systeme einsetzen, um Bedrohungen in Echtzeit zu erkennen und über Netzwerke und Geräte hinweg zu reagieren.

Management Summary

Im digitalen Zeitalter stehen Unternehmen vor der immerwährenden Herausforderung, ihre Betriebsgeheimnisse vor den wachsenden Bedrohungen zu schützen. Dabei sind Cyberangriffe nur ein - wenn auch relevantes – Szenario, wie die alarmierenden Ergebnisse der Bitkom-Umfrage 2024 zeigen. Insbesondere der Verlust sensibler Informationen rückt zunehmend in den Fokus. Während künstliche Intelligenz auch als Risikofaktor wahrgenommen wird, bieten **unerlässliche Sicherheitsstrategien und -technologien, wie etwa Threat Intelligence, Authentifizierungsmethoden und -verfahren, Data Loss Prevention oder Netzwerküberwachung, Wege, um diesem Risiko zu begegnen.**



Über valantic

valantic berät Unternehmen seit vielen Jahren kompetent und umfassend im Bereich der Cybersicherheit – vom Information Security Management über Regulatory Compliance bis hin zu präventiven Maßnahmen wie Threat Intelligence Analysen und Darknet Monitoring. So stellen wir sicher, dass unsere Kunden den Bedrohungen im digitalen Zeitalter einen Schritt voraus sind. Denn Sicherheit beginnt vor der Krise.

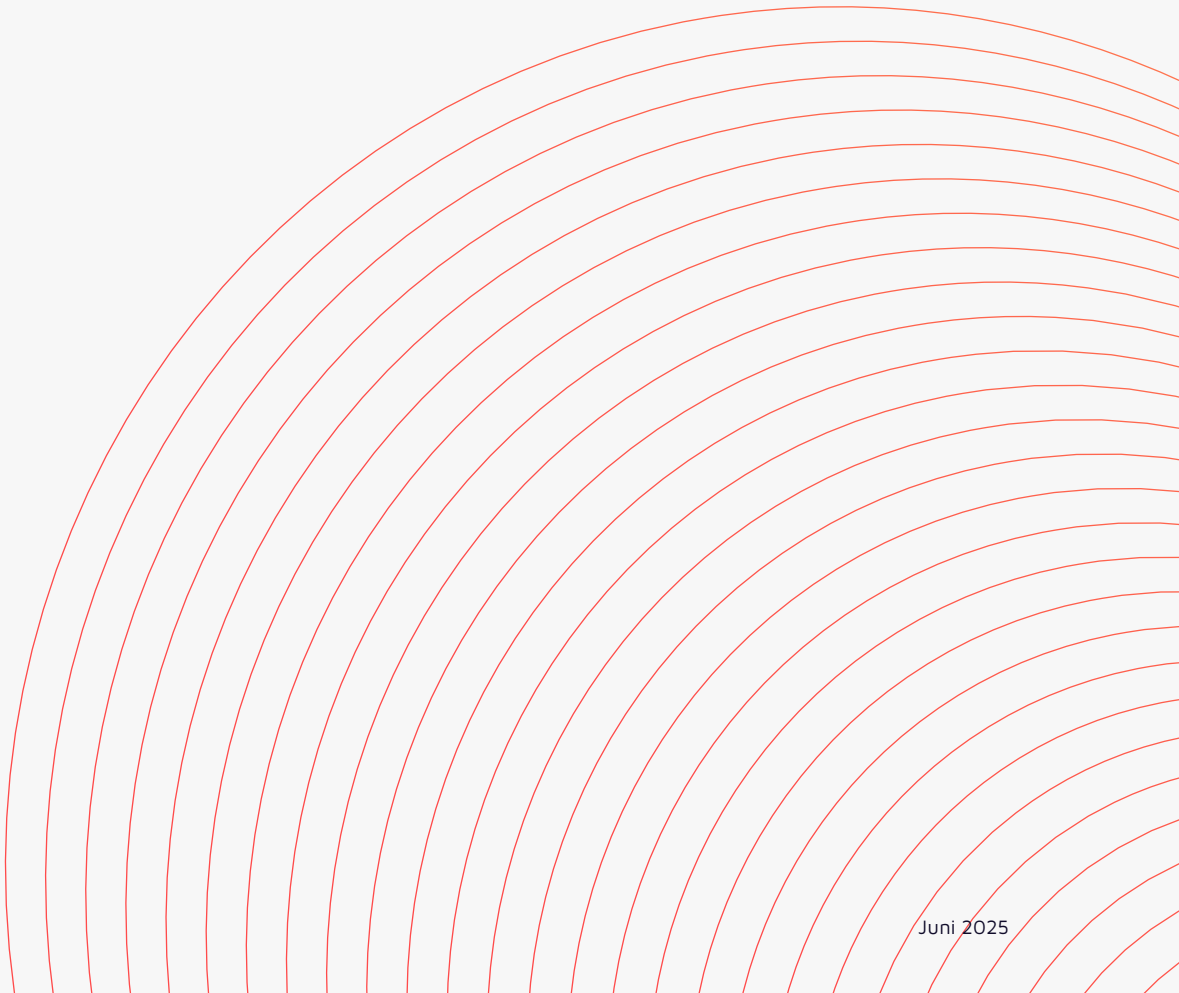
valantic

Kontakt

Dreieich Plaza 2A
63303 Dreieich
Deutschland

Telefon +49 6103 5086 0
info@mc.valantic.com

www.valantic.com



Juni 2025