SpaceNet

Cybersicherheit im Fokus:

Wie MSSP den Mittelstand effektiv schützen können

PERSÖNLICH.
STARK.
SICHER.
KLUG.
RICHTIG GUT.

Inhalt

Einleitung

Die digitale Bedrohungslage entwickelt sich rasant – und Unternehmen stehen zunehmend unter Druck, ihre IT-Sicherheit auf ein neues Niveau zu heben. Cyberangriffe werden nicht nur häufiger, sondern auch raffinierter. Während Cyberkriminelle automatisierte Angrifstools und künstliche Intelligenz nutzen, stehen viele Unternehmen vor einem ernüchternden Problem: Ihre IT-Abteilungen sind überlastet, es mangelt an Fachkräften, und die bestehenden Sicherheitsmaßnahmen reichen oft nicht mehr aus.

Trotz des steigenden Risikos fehlt es vielen mittelständischen Unternehmen an den Ressourcen, ein eigenes Security Operations Center (SOC) zu betreiben oder rund um die Uhr Cyberbedrohungen zu überwachen. Gleichzeitig steigen regulatorische Anforderungen wie die EU-Richtlinie NIS2, die Geschäftsführer und Vorstände stärker in die Verantwortung nimmt. Unternehmen müssen daher handeln – aber wie können sie ihre Sicherheitsarchitektur stärken, ohne ihr IT-Team zu überfordern?

Hier kommen Managed Security Service Provider (MSSP) ins Spiel. Sie bieten eine effiziente und kostengünstige Lösung, um IT-Sicherheitsaufgaben auszulagern, Bedrohungen frühzeitig zu erkennen und im Ernstfall schnell zu reagieren. Durch den Einsatz eines MSSP können Unternehmen rund um die Uhr auf modernste Sicherheitstechnologien und Expertenwissen zugreifen, ohne hohe Investitionen in eigene Infrastruktur oder Personal leisten zu müssen.

Dieses Whitepaper zeigt, warum IT-Sicherheit nicht mehr nur eine technische, sondern eine strategische Entscheidung ist – und wie Unternehmen mit einem MSSP ihre Cyberabwehr stärken, Compliance Anforderungen erfüllen und ihre IT-Ressourcen gezielt entlasten können.

1.0 Die aktuelle Bedrohungslage – Cyberangriffe auf den Mittelstand

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch	Schadensummen in MRD Euro (2024)	Schadensummen in MRD Euro (2023)	Schadensummen in MRD Euro (2022)
Ausfall, Diebstahl oder Schädigung von Infomations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.b. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen	14,8	10,4	18,8
Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	–
Sonstige Schäden	0	1,1	0,9
Gesamtschaden pro Jahr	**266,6**	**205,9**	**202,7**

Basis: Alle Unternehmen (n=1003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

1.1 Ein wachsendes Risiko für KMU und den Mittelstand

Die digitale Transformation bringt Unternehmen zahlreiche Vorteile, doch sie geht auch mit erheblichen Risiken einher. Besonders kleine und mittelständische Unternehmen (KMU) sowie der gehobene Mittelstand sind zunehmend Ziel von Cyberangriffen. Anders als Großkonzerne verfügen sie meist nicht über eigene Security-Teams oder ein Security Operations Center (SOC), was sie für Angreifer besonders attraktiv macht.

Statistiken zeigen die Dringlichkeit des Problems: Laut einer Bitkom-Studie wurden 81 % aller Unternehmen in Deutschland bereits Opfer eines Cyberangriffs – mit Schäden von über 266 Milliarden Euro [1].

Besonders besorgniserregend: Der Mittelstand ist immer häufiger direkt betroffen. Für KMU sind die Folgen oft existenzbedrohend. Ein Grund für die hohe Verwundbarkeit von Mittelständlern ist, dass viele Unternehmen ihre IT-Sicherheit bislang nicht als strategische Priorität betrachten. Während Großunternehmen über dedizierte Sicherheitsteams und hochmoderne Schutzmaßnahmen verfügen, setzen sich KMU oft nur sporadisch mit Cybersecurity auseinander. Angreifer wissen das und setzen gezielt auf Methoden, die mit wenig Aufwand maximale Schäden verursachen können.

Quelle: [1] – Wirtschaftsschutz 2024, Dr. Ralf Wintergerst, Bitkom, 28.08.2024

1.2 Die häufigsten Angriffsvektoren

Cyberkriminelle setzen auf verschiedene Methoden, um in Netzwerke einzudringen, Daten zu stehlen oder Unternehmen zu erpressen. Dabei haben sich insbesondere drei Angriffstechniken als besonders wirksam und weit verbreitet erwiesen: Phishing, Ransomware und DDoS-Angriffe. Diese Methoden sind nicht nur effektiv, sondern werden durch technologische Fortschritte und Automatisierung immer raffinierter.

Phishing – der digitale Türöffner für Angreifer

Phishing ist eine der ältesten, aber auch erfolgreichsten Cyberangriffsmethoden. Dabei täuschen Angreifer mit manipulierten E-Mails, SMS oder gefälschten Websites eine vermeintlich vertrauenswürdige Kommunikation vor, um an vertrauliche Daten zu gelangen oder Schadsoftware auf Unternehmenssystemen zu installieren.

Besonders Spear-Phishing ist gefährlich: Hier wird nicht wahllos an Tausende von Empfängern gesendet, sondern gezielt an bestimmte Personen oder Abteilungen im Unternehmen. Angreifer nutzen Informationen aus sozialen Netzwerken oder aus öffentlich zugänglichen Quellen, um ihre Nachrichten möglichst authentisch erscheinen zu lassen. Beispielsweise könnte eine täuschend echt aussehende E-Mail von einem vermeintlichen CEO an die Buchhaltung gesendet werden, mit der dringenden Aufforderung, eine Zahlung an einen neuen Lieferanten zu leisten.

Phishing ist deshalb so gefährlich, weil es nicht auf technische Sicherheitslücken abzielt, sondern auf den Menschen als Schwachstelle. Ein unachtsamer Klick kann reichen, um eine Schadsoftware zu installieren oder Angreifern Zugriff auf interne Systeme zu ermöglichen.

Ransomware – wenn Daten zur Geisel werden

Ransomware ist eine der lukrativsten Angriffsmethoden für Cyberkriminelle. Dabei verschlüsseln Angreifer die Daten eines Unternehmens und fordern ein Lösegeld, um sie wieder freizugeben. Oft werden dabei auch komplette IT-Infrastrukturen lahmgelegt, sodass Unternehmen nicht mehr auf ihre Systeme zugreifen können. Doppelte Erpressung (Double Extor-

tion) hat sich als gängige Methode etabliert: Neben der Verschlüsselung der Daten drohen Angreifer, gestohlene Informationen zu veröffentlichen. Diese Methode erhöht den Druck auf Unternehmen erheblich, da nicht nur der Verlust der Daten droht, sondern auch schwerwiegende Datenschutzverstöße und Reputationsschäden.

Moderne Ransomware-Angriffe nutzen "Ransomware-as-a-Service" (RaaS), ein Geschäftsmodell, bei dem Cyberkriminelle ihre Angriffe als Dienstleistung anbieten. Hierbei kann sich praktisch jeder – ohne großes technisches Wissen – eine Ransomware-Kampagne starten lassen und einen Teil des erpressten Lösegelds mit den Entwicklern der Schadsoftware teilen.

Die Folgen eines Ransomware-Angriffs sind weitreichend. Neben dem finanziellen Schaden durch Lösegeldzahlungen und Betriebsausfälle sind auch Kosten für forensische Analysen, Wiederherstellung der IT-Systeme und rechtliche Auseinandersetzungen erheblich.

So stellt Sophos im Report The State of Ransomware 2024 eine durchschnittliche Wiederherstellungszeit von ungefähr einem Monat fest [2]. Eine Zeitspanne, die für viele mittelständische Unternehmen das Permanente Aus bedeuten würde.

DDoS-Angriffe – gezielte Überlastung der IT

Während Phishing und Ransomware auf den direkten finanziellen Schaden abzielen, verfolgen Distributed-Denial-of-Service (DDoS)-Angriffe eine andere Taktik: Sie legen IT-Systeme lahm, indem sie Server oder Netzwerke mit massiven Anfragen überlasten.

Dabei nutzen Angreifer oft Botnetze, also Netzwerke aus Tausenden oder Millionen infizierter Computer und IoT-Geräte, die gleichzeitig Anfragen an ein bestimmtes Ziel senden.

Unternehmen, die von einem DDoS-Angriff getroffen werden, verlieren nicht nur Umsätze durch den Ausfall von Webshops oder Online-Diensten, sondern riskieren auch langfristige Kundenverluste durch die eingeschränkte Erreichbarkeit.

Eine besonders raffinierte Methode ist der Application-Layer-DDoS-Angriff, bei dem nicht einfach massenhafte Verbindungsanfragen erzeugt werden, sondern gezielt Applikationen attackiert werden.

Ein Beispiel ist die Manipulation von Login-Seiten oder Datenbankabfragen, wodurch Systeme überlastet und funktionsunfähig gemacht werden.

Zunehmend werden DDoS-Angriffe auch als Ablenkungsmanöver eingesetzt. Während die IT-Abteilung mit der Abwehr eines DDoS-Angriffs beschäftigt ist, nutzen Angreifer die Gelegenheit, um in Systeme einzudringen, Daten zu exfiltrieren oder Ransomware zu platzieren.

Quelle: [2] – Ransomware-Report 2024, Sophos, April 2024

1.3 Regulatorische Anforderungen und Compliance

Die zunehmende Bedrohung durch Cyberangriffe hat nicht nur Auswirkungen auf Unternehmen selbst, sondern auch auf den Gesetzgeber. In den vergangenen Jahren wurden zahlreiche neue Regulierungen eingeführt, um Unternehmen dazu zu verpflichten, angemessene Sicherheitsmaßnahmen zu ergreifen.

Besonders die EU-Richtlinien NIS2 und DORA sowie der internationale Sicherheitsstandard ISO 27001:2022 setzen neue Maßstäbe für Cybersicherheit. Diese Vorgaben betreffen nicht nur Großunternehmen, sondern zunehmend auch den Mittelstand.

Wer die neuen Vorschriften nicht einhält, riskiert hohe Bußgelder und haftungsrechtliche Konsequenzen für Geschäftsführungen und Vorstände.

NIS2 – Neue Verpflichtungen für Unternehmen in Europa

Die Network and Information Security Directive 2 (NIS2) ist die überarbeitete Version der ursprünglichen NIS-Richtlinie, die 2016 eingeführt wurde. Die neue Version trat 2024 in Kraft und zielt darauf ab, die Cybersicherheitsstandards in der gesamten EU zu verbessern.

Wer ist betroffen?

Während die ursprüngliche NIS-Richtlinie nur bestimmte „kritische Infrastrukturen" wie Energieversorger oder Telekommunikationsanbieter umfasste, erweitert NIS2 den Geltungsbereich erheblich. Nun fallen auch mittelständische Unternehmen in wichtigen Wirtschaftssektoren unter die Regelung. Dazu gehören:

> Produzierendes Gewerbe (z. B. Maschinenbau, Automobilindustrie)
> Gesundheitswesen (Krankenhäuser, Pharmaunternehmen)
> Digitale Infrastrukturen (Cloud-Dienste, Rechenzentren)
> Transport & Logistik
> Finanzdienstleistungen & Versicherungen

Diese Unternehmen sind verpflichtet, ein umfangreiches Cybersicherheits- und Risikomanagement einzuführen.

Was fordert die NIS2-Richtlinie?

Die Kernforderungen von NIS2 umfassen:

> Striktere Risikomanagementprozesse: Unternehmen müssen nachweisen, dass sie IT-Risiken systematisch bewerten und Gegenmaßnahmen ergreifen.
> Schnelle Meldung von Cyberangriffen: Sicherheitsvorfälle müssen innerhalb von 24 Stunden gemeldet werden. Eine vollständige Analyse muss spätestens nach 72 Stunden vorliegen.
> Haftung von Führungskräften: Geschäftsführungen und Vorstände können bei mangelnder Sicherheitsvorsorge persönlich haftbar gemacht werden.
> Strenge Strafen: Verstöße gegen NIS2 können mit Bußgeldern von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes geahndet werden.

Besonders die persönliche Haftung von Führungskräften ist eine deutliche Verschärfung gegenüber früheren Regelungen. Unternehmen müssen nun nachweisen, dass ihre Sicherheitsmaßnahmen nicht nur existieren, sondern auch regelmäßig geprüft und verbessert werden.

DORA – Cyber-Resilienz für den Finanzsektor

Der Digital Operational Resilience Act (DORA) ist eine EU-Verordnung, die speziell für Finanzinstitute und deren IT-Dienstleister gilt. Die Verordnung zielt darauf ab, die Widerstandsfähigkeit des Finanzsektors gegenüber Cyberangriffen zu erhöhen.

Wer ist betroffen?

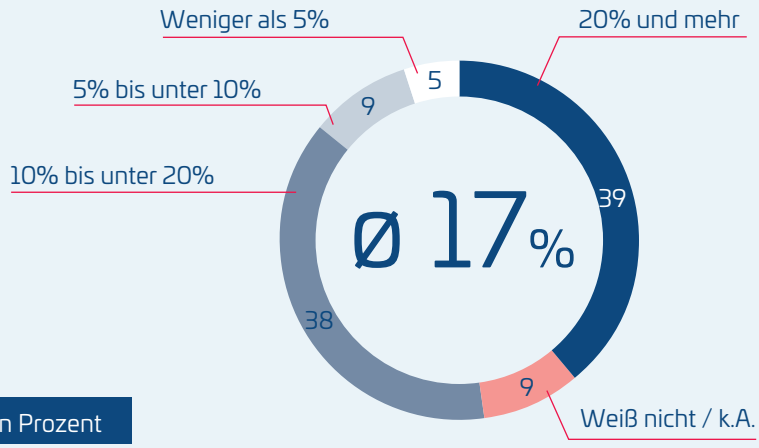
DORA gilt für:

> Banken & Sparkassen
> Versicherungen & Rückversicherer
> Zahlungsdienstleister & Kreditinstitute
> IT-Dienstleister, die Finanzunternehmen unterstützen

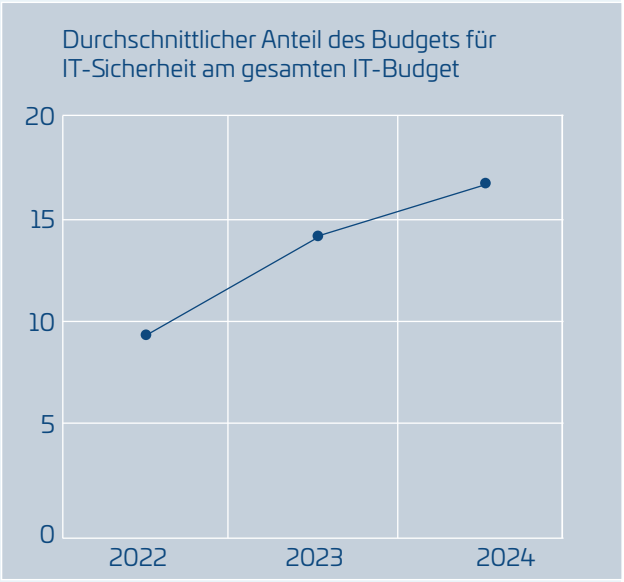
Da der Finanzsektor eine hohe Abhängigkeit von digitalen Systemen hat, hat die EU mit DORA strengere Sicherheitsanforderungen geschaffen, um systemische Risiken zu minimieren.

Cybersicherheit: Investionsbereitschaft steigt

Wie hoch ist geschätzt der Anteil des Budgetes für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens



In Prozent



Basis: Alle Unternehmen (n_1003) | Quelle: Bitkom Research 2024

Welche Anforderungen stellt DORA?

Die Verordnung verlangt unter anderem:

> Umfassende Sicherheits- und Krisenpläne: Unternehmen müssen detaillierte Business-Continuity-Pläne für den Fall eines Cyberangriffs haben.
> Regelmäßige Stresstests: IT-Systeme müssen regelmäßig auf ihre Belastbarkeit bei Cyberangriffen geprüft werden.
> Striktes Monitoring von Drittanbietern: IT-Dienstleister, die mit Banken oder Versicherungen zusammenarbeiten, müssen ebenfalls strenge Sicherheitsauflagen erfüllen.
> Zentrale EU-Überwachung: Finanzaufsichtsbehörden können IT-Dienstleister und Finanzunternehmen überwachen und bei Sicherheitsmängeln Maßnahmen ergreifen.

Für Finanzunternehmen bedeutet dies eine deutliche Verschärfung der bisherigen Anforderungen. Besonders die Verpflichtung zu regelmäßigen Stresstests und die Meldepflicht für Sicherheitsvorfälle erhöhen den Druck auf IT-Abteilungen.

ISO 27001: 2022 – Der internationale Sicherheitsstandard

Neben den EU-Richtlinien gewinnt auch der internationale Standard ISO/IEC 27001:2022 an Bedeutung. Diese Norm beschreibt, wie Unternehmen ein Informationssicherheits-Managementsystem (ISMS) implementieren können, um Cyberrisiken zu minimieren.

Warum ist ISO 27001 wichtig?

> Zertifizierung als Wettbewerbsvorteil: Viele Unternehmen verlangen von Geschäftspartnern eine ISO 27001-Zertifizierung als Nachweis für eine robuste Sicherheitsstrategie.
> Anpassung an aktuelle Bedrohungen: Die überarbeitete Version von 2022 enthält neue Anforderungen zu Cloud-Sicherheit, Risikomanagement und Schutz vor Cyberangriffen.
> Vermeidung von Datenpannen: Ein systematisches Sicherheitsmanagement reduziert das Risiko von Datenschutzverletzungen und deren finanzielle Folgen.

Welche Neuerungen enthält ISO 27001:2022?

> Erweiterte Risikobewertung: Unternehmen müssen Schwachstellen regelmäßig bewerten und dokumentieren, wie sie Sicherheitsrisiken minimieren.
> Sicherheit von Cloud-Diensten: Da immer mehr Unternehmen Cloud-Lösungen nutzen, wurde ein besonderer Fokus auf den Schutz von Cloud-Umgebungen gelegt.
> Zero-Trust-Ansatz: Die Norm empfiehlt Sicherheitsstrategien, die auf dem Prinzip „Vertraue niemandem, überprüfe alles“ basieren.

Was bedeutet die Zertifizierung für Unternehmen?
Die Zertifizierung nach ISO 27001 ist kein einmaliges Projekt, sondern ein kontinuierlicher Verbesserungsprozess. Unternehmen müssen regelmäßig nachweisen, dass sie ihre Sicherheitsmaßnahmen auf dem neuesten Stand halten.

Warum Unternehmen jetzt handeln müssen
Die Einführung von NIS2, DORA und die Weiterentwicklung der ISO 27001-Norm zeigen, dass Cybersicherheit nicht mehr optional ist – sie wird zur gesetzlichen Pflicht. Besonders für mittelständische Unternehmen bedeutet dies, dass sie sich frühzeitig mit den neuen Anforderungen auseinandersetzen müssen, um:

> Hohe Bußgelder und rechtliche Konsequenzen zu vermeiden
> Sicherheitslücken zu schließen, bevor es zu einem Angriff kommt
> Vertrauen bei Kunden und Partnern zu stärken

Die Einhaltung dieser Vorschriften ist keine reine Compliance-Aufgabe – sie trägt aktiv dazu bei, Unternehmen gegen die wachsende Bedrohungslage zu schützen.

Wer sich frühzeitig auf die neuen Anforderungen vorbereitet und ein effektives Sicherheitsmanagement implementiert, reduziert nicht nur das eigene Risiko, sondern kann sich auch als verlässlicher und sicherer Geschäftspartner positionieren.

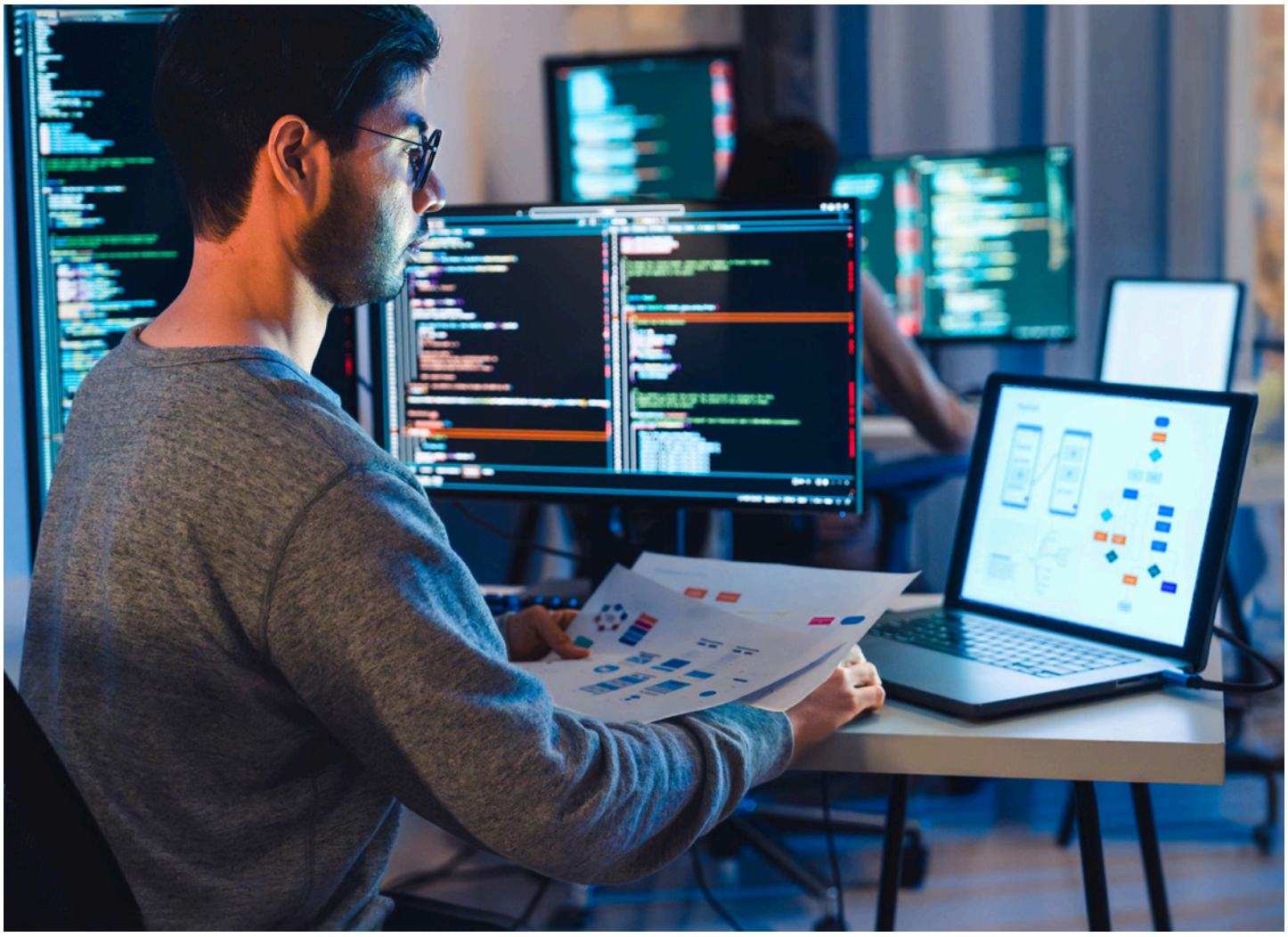
2.0 Herausforderungen für Unternehmen – Warum Cybersicherheit für viele Betriebe schwer umsetzbar ist

IT-Sicherheit ist heute eine der größten Herausforderungen für Unternehmen. Während Cyberangriffe immer raffinierter werden und gesetzliche Anforderungen steigen, kämpfen viele Betriebe mit internen Hürden, die eine wirksame Sicherheitsstrategie erschweren. Besonders drei Faktoren machen es Unternehmen schwer, angemessene Schutzmaßnahmen zu etablieren:

1. Fachkräftemangel – Es gibt zu wenige IT-Security-Experten auf dem Markt.
2. Hohe Kosten – Der Aufbau und Betrieb einer eigenen Sicherheitsinfrastruktur ist für viele Unternehmen finanziell nicht tragbar.
3. Komplexität – Sicherheitsrisiken sind schwer zu identifizieren und zu managen.

Diese Herausforderungen treffen vor allem den Mittelstand, da größere Konzerne oft über mehr finanzielle Mittel und Personal verfügen. Doch auch kleinere Unternehmen müssen sich gegen Cyberangriffe absichern – und stehen dabei oft vor unlösbar erscheinenden Problemen.

2.1 Der Fachkräftemangel in der IT-Sicherheit – Experten sind Mangelware



Einer der größten Engpässe in der Cybersicherheit ist der akute Fachkräftemangel. Während Unternehmen zunehmend auf IT-Sicherheit angewiesen sind, fehlen ihnen schlicht die Experten, um diese Aufgabe zu bewältigen.

Wie groß ist der Mangel an IT-Sicherheitsexperten?

> Laut einer Studie des Branchenverbands Bitkom fehlten schon 2023 in Deutschland rund 149.000 IT-Fachkräfte, viele davon im Bereich IT-Sicherheit [3].

Warum gibt es so wenige IT-Security-Experten?

> Hohe Spezialisierung erforderlich: IT-Sicherheitsprofis müssen sich mit Netzwerksicherheit, Bedrohungserkennung, Compliance-Vorgaben und Incident-Response-Strategien auskennen.
> Nachfrage übersteigt das Angebot: Der Markt wächst schneller als die Zahl der ausgebildeten Fachkräfte.
> Konkurrenz durch Großunternehmen: Große Konzerne locken Talente mit hohen Gehältern, was es mittelständischen Unternehmen schwer macht, qualifizierte IT-Security-Spezialisten zu gewinnen.

Die Folge:

Viele Unternehmen müssen ihre IT-Sicherheit mit überlasteten IT-Teams stemmen, die ohnehin schon mit Infrastrukturwartung und Software-Management ausgelastet sind. Eine spezialisierte Security-Überwachung rund um die Uhr ist so kaum realisierbar.

Quelle: [3] – Mangel an IT-Fachkräften droht sich dramatisch zu verschärfen, Bitkom, 11.04.2024

2.2 Die hohen Kosten für IT-Sicherheitsinfrastruktur

Die digitale Transformation eröffnet Unternehmen die Möglichkeit, neue Geschäftsmodelle zu entwickeln. Datengetriebene Ansätze, digitale Plattformen und kundennahe Services sind eng mit einer modernen IT-Infrastruktur verknüpft. Nur wer seine IT zukunftssicher aufstellt, kann das volle Potenzial digitaler Innovationen ausschöpfen und sich nachhaltig im Wettbewerb positionieren.

Wie teuer ist eine eigene Sicherheitsarchitektur?

Ein vollständiges IT-Sicherheitskonzept umfasst:

> Firewalls und Intrusion Detection Systeme (IDS/IPS) zur Netzwerküberwachung
> Security Information and Event Management (SIEM)-Lösungen zur Erkennung von Bedrohungen
> Endpoint Detection & Response (EDR)-Technologien für den Schutz von Arbeitsplätzen und Servern
> Regelmäßige Penetrationstests zur Überprüfung der Sicherheitsmaßnahmen
> Security Operations Center (SOC) zur kontinuierlichen Überwachung und Incident Response

Ein kleines bis mittelständisches Unternehmen müsste für eine solche Sicherheitsstruktur mehrere hunderttausend Euro pro Jahr investieren.

Selbst Unternehmen, die sich für eine hybride Lösung mit internen und externen Sicherheitsdienstleistungen entscheiden, müssen hohe Budgets einplanen. Lizenzgebühren für Sicherheitssoftware, regelmäßige Updates und die Schulung von Mitarbeitenden erhöhen die laufenden Kosten zusätzlich.

Für viele Mittelständler ist diese Investition schlicht nicht realisierbar – was sie in eine gefährliche Lage bringt. Ohne ausreichenden Schutz setzen sie sich einem enormen Risiko aus: Die Kosten eines erfolgreichen Cyberangriffs können ein Vielfaches höher sein als präventive Sicherheitsmaßnahmen. Unternehmen, die nicht in Cybersicherheit investieren, setzen sich also einem finanziellen Risiko aus, das im schlimmsten Fall existenzbedrohend sein kann.

2.3 Die Komplexität des Cybersicherheits-managements – Unternehmen kämpfen mit Überforderung

Neben dem Fachkräftemangel und den hohen Kosten kommt ein weiteres Problem hinzu: Die Verwaltung von IT-Sicherheit ist extrem komplex. Selbst Unternehmen, die in Sicherheits-maßnahmen investieren, haben oft damit zu kämpfen, Cyber-risiken proaktiv zu managen.

Warum ist IT-Sicherheitsmanagement so schwierig?

> Dynamische Bedrohungslage: Cyberkriminelle entwickeln ständig neue Angriffsmethoden. Unternehmen müssen mit dieser rasanten Entwicklung Schritt halten, was regel-mäßige Schulungen und Investitionen in neue Techno-logien erfordert.

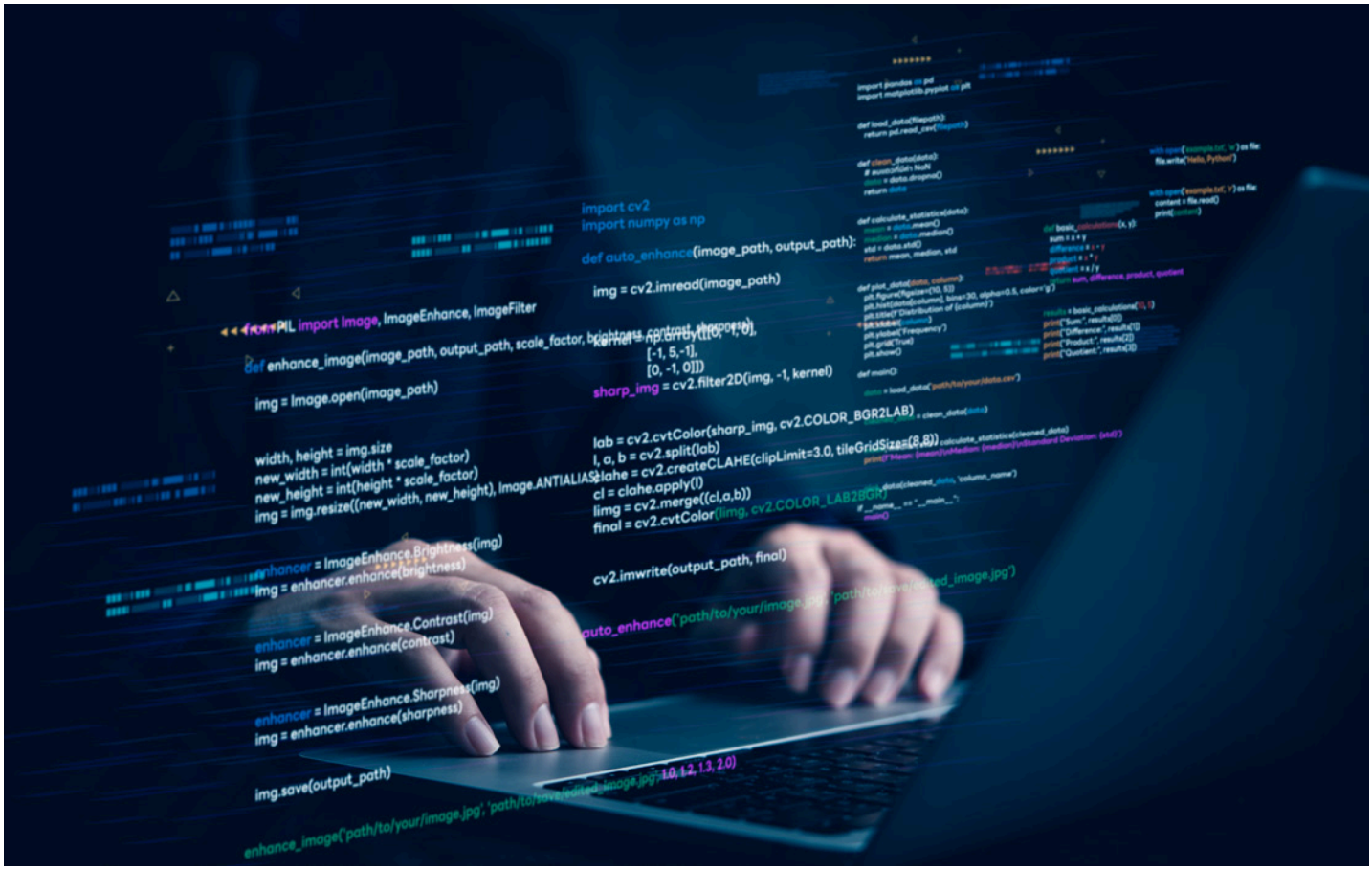
> Fehlendes Sicherheitsbewusstsein: Viele Mitarbeitende sind sich der Risiken nicht bewusst und handeln unab-sichtlich fahrlässig. Ein unachtsam geöffnetes Phishing-Mail kann ausreichen, um Schadsoftware ins Unterneh-mensnetzwerk einzuschleusen.

> Komplexe Compliance-Anforderungen: Unternehmen müssen nicht nur ihre IT-Systeme schützen, sondern auch gesetzliche Vorgaben einhalten. Die Umsetzung von NIS2, DORA oder ISO 27001 erfordert detaillierte Doku-mentation, regelmäßige Audits und interne Schulungen.

Fehlende Angriffserkennung als großes Problem

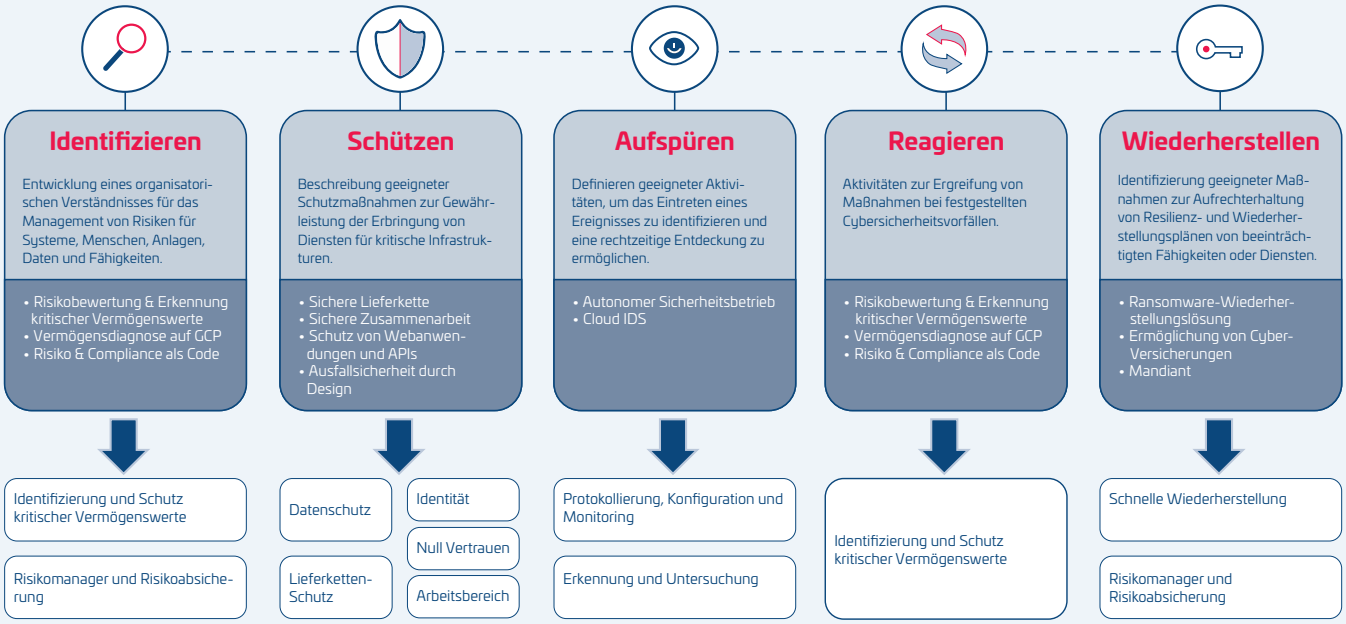
Ein besonders kritischer Aspekt ist die Fähigkeit, Cyber-angriffe rechtzeitig zu erkennen. Laut IBM dauert es im Durchschnitt 277 Tage, bis ein Sicherheitsvorfall entdeckt wird [4]. Viele Angriffe laufen monatelang unbemerkt im Hintergrund, während Hacker Daten exfiltrieren oder sich Zugang zu Unternehmensnetzwerken verschaffen.

Unternehmen, die keine Security Operations Center (SOC) oder Managed Detection & Response (MDR)-Lösungen nutzen, haben oft keine Möglichkeit, verdächtige Aktivitäten in Echtzeit zu erkennen. Dies führt dazu, dass Sicherheits-vorfälle erst bemerkt werden, wenn bereits erheblicher Schaden entstanden ist.



Quelle: [4] – data security report 2022, IBM security, 2022

3.0 Managed Security Services als Lösung



3.1: Was ist ein MSSP und welche Vorteile bietet er?

In den vorherigen Kapiteln wurde deutlich, dass Unternehmen vor großen Herausforderungen im Bereich der IT-Sicherheit stehen: Fachkräftemangel, hohe Kosten für eine eigene Sicherheitsinfrastruktur und die zunehmende Komplexität von Cyberbedrohungen. Viele Unternehmen, insbesondere KMU und der Mittelstand, können diese Hürden kaum allein bewältigen. Hier setzt das Konzept eines Managed Security Service Providers (MSSP) an.

Was ist ein MSSP?

Ein Managed Security Service Provider (MSSP) ist ein externer Dienstleister, der Unternehmen dabei unterstützt, ihre IT-Sicherheitsstrategie zu optimieren und kontinuierlich zu überwachen. MSSPs übernehmen verschiedene sicherheitsrelevante Aufgaben, darunter:

> Überwachung der IT-Infrastruktur rund um die Uhr (24/7 Monitoring)
> Erkennung und Abwehr von Cyberangriffen (Threat Detection & Response)
> Sicherheitsanalysen und Schwachstellenmanagement
> Compliance- und Risikomanagement gemäß gesetzlicher Anforderungen
> Incident Response und Forensik im Falle eines Angriffs
> Sicherheitsberatung und strategische Weiterentwicklung der IT-Sicherheit

Ein MSSP agiert also wie eine externe Sicherheitszentrale, die Unternehmen entlastet und deren IT-Abteilungen mit Fachwissen und modernster Technologie unterstützt.

Welche Vorteile bietet ein MSSP?

Die Auslagerung von IT-Sicherheitsaufgaben an einen MSSP bringt zahlreiche Vorteile mit sich, die Unternehmen dabei helfen, ihre Cybersicherheit effizienter und kostengünstiger zu gestalten.

1. RUND-UM-DIE-UHR-ÜBERWACHUNG UND SCHNELLERE REAKTIONSZEITEN

Cyberangriffe erfolgen oft außerhalb der regulären Arbeitszeiten – an Wochenenden oder in den Nachtstunden. Während viele Unternehmen kein 24/7-Sicherheitsteam unterhalten können, bieten MSSPs eine kontinuierliche Überwachung der IT-Systeme. Verdächtige Aktivitäten werden in Echtzeit erkannt und Sicherheitsmaßnahmen automatisch oder durch Experten eingeleitet.

2. ZUGANG ZU EXPERTENWISSEN UND NEUESTEN TECHNOLOGIEN

Da qualifizierte IT-Security-Experten Mangelware sind, profitieren Unternehmen durch einen MSSP von hochspezialisiertem Fachwissen, ohne selbst Mitarbeiter rekrutieren zu müssen. MSSPs verfügen über:

> Sicherheitsanalysten und Incident-Response-Teams, die Bedrohungen analysieren
> Threat-Intelligence-Plattformen, die neue Cyberbedrohungen frühzeitig erkennen
> Erfahrungen mit aktuellen Angriffsszenarien, um Unternehmen proaktiv zu schützen

3. REDUZIERUNG DER KOSTEN FÜR IT-SICHERHEIT

Der Aufbau einer eigenen IT-Sicherheitsinfrastruktur ist teuer. MSSPs bieten skalierbare Lösungen, die Unternehmen individuell anpassen können.

> Kostenvorteile durch Shared Services: MSSPs betreiben Security-Operation-Center (SOC) für mehrere Kunden und ermöglichen dadurch kosteneffiziente Sicherheitsdienste
> Flexible Preismodelle: Unternehmen zahlen nur für die Services, die sie wirklich benötigen

4. EINHALTUNG REGULATORISCHER ANFORDERUNGEN (COMPLIANCE)

Mit der Einführung von NIS2, DORA und ISO 27001:2022 stehen Unternehmen unter wachsendem Druck, gesetzliche Sicherheitsanforderungen zu erfüllen. MSSPs unterstützen Unternehmen bei der Umsetzung und Überprüfung dieser Vorgaben, indem sie:

> Regelmäßige Audits und Sicherheitsberichte bereitstellen
> Meldepflichten für Sicherheitsvorfälle automatisieren (z. B. innerhalb von 24 Stunden gemäß NIS2)
> Technische und organisatorische Sicherheitsmaßnahmen implementieren

5. SKALIERBARKEIT UND FLEXIBILITÄT

Unternehmen wachsen und verändern sich – und damit auch ihre Anforderungen an die IT-Sicherheit. MSSPs bieten skalierbare Lösungen, die je nach Bedarf erweitert oder reduziert werden können.

> Start-ups und KMU: Können mit Basis-Sicherheitsservices beginnen und diese mit zunehmendem Wachstum erweitern.
> Mittelständische Unternehmen: Können gezielt einzelne Sicherheitsbereiche auslagern, etwa das 24/7-Monitoring oder die Incident Response.
> Großunternehmen: Können MSSPs als Ergänzung zu ihrem eigenen Security-Team nutzen, um spezifische Aufgaben (z. B. Penetrationstests) auszulagern.

6. VERBESSERTE REAKTIONSFÄHIGKEIT BEI SICHERHEITSVORFÄLLEN

Ein MSSP hilft Unternehmen nicht nur bei der Prävention von Angriffen, sondern auch bei der schnellen Reaktion im Ernstfall. Durch vordefinierte Incident-Response-Prozesse und ein erfahrenes Team kann der Schaden bei einem Sicherheitsvorfall erheblich reduziert werden.

4.0 SpaceNet als MSSP – ein Praxisbeispiel

Ausgangssituation

Ein mittelständisches Unternehmen aus der Fertigungsbranche sah sich mit den neuen Compliance-Vorgaben der NIS2-Richtlinie konfrontiert. Die regulatorischen Anforderungen an IT-Sicherheit und Resilienz wurden verschärft, wodurch das Unternehmen gezwungen war, seine Sicherheitsstrategie zu überarbeiten. Die vorhandenen IT-Ressourcen waren stark ausgelastet, und es fehlte an spezialisiertem Know-how, um Bedrohungen effektiv abzuwehren und gesetzliche Vorgaben zu erfüllen. Gleichzeitig sollte der Aufwand für die interne IT minimal bleiben, um sich weiterhin auf das Kerngeschäft konzentrieren zu können.

Die Lösung: SpaceNet als Managed Security Service Provider (MSSP)

SpaceNet wurde als MSSP beauftragt, um die Sicherheitsarchitektur zu optimieren und die neuen NIS2-Compliance-Anforderungen effizient umzusetzen. Eine zentrale Rolle spielte dabei das SpaceNet Security Operations Center (SOC), das rund um die Uhr Bedrohungen analysiert und abwehrt. Durch eine gezielte Analyse der bestehenden IT-Infrastruktur entwickelte SpaceNet ein individuelles Sicherheitskonzept mit folgenden Kernkomponenten:

> SpaceNet SOC: 24/7-Überwachung und Bedrohungsanalyse zur frühzeitigen Erkennung und Abwehr von Angriffen.
> Managed SIEM (Security Information and Event Management): Implementierung einer Echtzeit-Analyse von Sicherheitsereignissen zur proaktiven Bedrohungserkennung.
> Endpoint Detection & Response (EDR): Schutz der Endgeräte durch KI-gestützte Erkennung und Abwehr von Angriffen.
> Security Awareness Training: Schulung der Mitarbeitenden, um menschliche Fehler als Einfallstor für Cyberangriffe zu minimieren.
> Compliance-Management: Sicherstellung der Einhaltung der NIS2-Vorgaben durch kontinuierliche Audits, Dokumentation und Berichterstattung.

Ergebnis und Mehrwert

Dank der Zusammenarbeit mit SpaceNet konnte das Unternehmen:

> Die Sicherheitslage erheblich verbessern, indem Cyberangriffe frühzeitig erkannt und abgewehrt wurden.
> Die internen IT-Ressourcen entlasten, da das SpaceNet SOC rund um die Uhr Monitoring übernahm.
> Die neuen NIS2-Compliance-Vorgaben nahtlos erfüllen, ohne zusätzlichen Verwaltungsaufwand.
> Die Sicherheit der IT-Systeme kontinuierlich verbessern, ohne hohe Investitionen in eigene Security-Teams.

Die Partnerschaft mit SpaceNet ermöglichte es dem Mittelständler, sich voll und ganz auf das Kerngeschäft zu konzentrieren, während Security und Compliance in den Händen von Experten lagen.

5.0 Handlungsempfehlungen und Next Steps

1. Rund-um-die-Uhr-Überwachung Ihrer IT-Sicherheit

> Wird Ihre IT-Infrastruktur 24/7 auf Angriffe überwacht – auch nachts und an Wochenenden? ☐

> Können Sicherheitsvorfälle in Echtzeit erkannt und abgewehrt werden? ☐

2. Frühzeitige Erkennung und Abwehr von Cyberangriffen

> Nutzen Sie ein Security Information and Event Management (SIEM)-System zur Analyse verdächtiger Aktivitäten? ☐

> Werden regelmäßig Penetrationstests durchgeführt, um Schwachstellen zu finden, bevor Angreifer es tun? ☐

3. Schutz vor Ransomware und Phishing

> Sind Ihre Mitarbeitenden regelmäßig in Phishing-Abwehr und IT-Sicherheitsbewusstsein geschult? ☐

> Sind Ihre Backups gegen Ransomware abgesichert und können schnell wiederhergestellt werden? ☐

4. Verfügbarkeit von IT-Security-Experten

> Haben Sie genügend interne Ressourcen, um Cyberangriffe zu analysieren und abzuwehren? ☐

5. Compliance und gesetzliche Vorgaben (NIS2, DORA, ISO 27001)

> Sind Sie auf gesetzliche Sicherheitsanforderungen vorbereitet, um hohe Strafen zu vermeiden? ☐

> Können Sie im Falle eines Angriffs innerhalb von 24 Stunden eine Meldung gemäß NIS2 abgeben? ☐

6. Notfall- und Incident-Response-Plan

> Gibt es einen detaillierten Notfallplan für Cyberangriffe, den Ihr Team kennt und umsetzen kann? ☐

> Wird dieser Plan regelmäßig getestet? ☐

7. Schutz gegen DDoS- und gezielte Angriffe

> Haben Sie Schutzmaßnahmen gegen DDoS-Angriffe, die Ihre Systeme lahmlegen könnten? ☐

> Wird verdächtiger Netzwerkverkehr automatisch gefiltert und abgewehrt? ☐

8. IT-Sicherheit als planbare Investition

> Haben Sie eine klare Kostenübersicht über Ihre IT-Sicherheitsmaßnahmen? ☐

> Können Sie hohe Einmalkosten vermeiden und IT-Sicherheit flexibel skalieren? ☐

9. Transparenz über aktuelle Sicherheitsbedrohungen

> Haben Sie Zugriff auf tagesaktuelle Bedrohungsanalysen, um neue Risiken frühzeitig zu erkennen? ☐

> Wird Ihr Sicherheitskonzept regelmäßig an neue Bedrohungen angepasst? ☐

10. Skalierbarkeit und Zukunftssicherheit Ihrer IT-Sicherheitsstrategie

> Ist Ihre IT-Sicherheitsstrategie an das Wachstum Ihres Unternehmens anpassbar? ☐

> Können Sie flexibel neue Sicherheitslösungen implementieren, wenn sich Anforderungen ändern? ☐