— Cybersicherheit für KMU in Baden-Württemberg

Erkenntnisse aus den Cybersecurity-Checkups des Projekts InnoSecBW

Version: 1.0
Veröffentlichung: 30.06.2024
Bearbeitet von: Marc Nemes, Akim Stark

– Inhaltsverzeichnis

Kurzzusammenfassung

Auch kleine und mittlere Unternehmen (KMU) werden Opfer von (automatisierten) Cyberangriffen, obwohl viele der erfolgreichen Angriffe vermeidbar wären. Im Rahmen des vom Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg geförderten Projekts *InnoSecBW* hat das FZI Forschungszentrum Informatik untersucht, in welchen Bereichen die größten Mängel existieren. Durch Kenntnis der häufigsten Mängel können in diesen Bereich verstärkt Präventionsangebote angeboten werden, um KMU besser vor Angriffen zu schützen. Zu diesem Zweck wurde im Rahmen des Projekts InnoSecBW ein Fragebogen mit 38 Fragen zu verschiedenen Sicherheitsvorkehrungen entwickelt und 20 KMU aus Baden-Württemberg zum Ist-Stand in ihrem Unternehmen befragt. Die Fragen decken ein breites Spektrum aus organisatorischen, technischen, physischen und innovativen Bereichen ab. Die Auswertung hat gezeigt, dass die meisten Unternehmen insbesondere bei organisatorischen Maßnahmen schlechter aufgestellt sind als bei technischen Maßnahmen. Eine Empfehlung ist daher insbesondere kleinen und mittlere Unternehmen auf die Wichtigkeit organisatorischer Maßnahmen hinzuweisen und entsprechende Unterstützungsangebote auszubauen.

1 Einleitung

Kleine und mittlere Unternehmen aus Baden-Württemberg konnten sich während der Laufzeit des Projekts *InnoSecBW* auf die Durchführung von C*ybersecurity-Checkups* und *Cybersecurity-Booster* bewerben. Diese Transferformate für Cybersicherheit in KMU wurden von Mitarbeitenden des FZI Forschungszentrum Informatik konzipiert und durchgeführt. Das Projekt InnoSecBW wurde von November 2022 bis Juni 2024 vom Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg gefördert.

Im vorliegenden Whitepaper werden die Erkenntnisse der im Rahmen von InnoSecBW durchgeführten Cybersecurity-Checkups vorgestellt.

Für die Konzeption der Cybersecurity-Checkups wurden zunächst anhand öffentlicher Quellen (u.a. Top 10 Sicherheitsrisiken des BSI oder OWASP) die am häufigsten genannten Schwachstellen und Gegenmaßnahmen gesammelt und nach Kategorien gruppiert in einem Fragebogen zusammengefasst. Der Fragebogen umfasste insgesamt 38 Fragen von denen 30 mit Ja oder Nein zu beantworten waren. Bei den übrigen 8 Fragen handelte es sich um Fragen mit Freitextantworten.

Während der Projektlaufzeit konnten sich KMU aus Baden-Württemberg auf die Durchführung eines Cybersecurity-Checkups über die Projektwebseite bewerben. Die Durchführung der Cybersecurity-Checkups erfolgte im Rahmen von 60 bis 90-minütige Videokonferenzen mit den IT-Verantwortlichen der jeweiligen Unternehmen. Dabei waren stets zwei Mitarbeitende des FZI Forschungszentrum Informatik anwesend, von denen ein Mitarbeiter das Gespräch geführt und die Fragen gestellt hat, während der andere Mitarbeiter sich ausschließlich auf das Ausfüllen des Fragebogens und protokollieren konzentriert hat. Aufgabe des Protokollanten war somit aus den Antworten der IT-Verantwortlichen herauszuhören, ob bestimmte Maßnahmen im Unternehmen effektiv umgesetzt werden oder nicht, und dementsprechend die passende Einschätzung niederzuschreiben. Zusätzlich hat der Protokollant am Ende jeder Frage bewertet, wie gut das Unternehmen in diesem Punkt vor Angriffen geschützt ist bzw. wie viel das Unternehmen hier verbessern kann. Die Bewertung erfolgte auf der folgenden Skala:

1. Enormes Verbesserungspotenzial
2. Viel Verbesserungspotenzial
3. Durchschnittlich
4. Etwas Verbesserungspotenzial
5. Optimal

Zusätzlich konnte die Option "Keine Einschätzung" gewählt werden. Um Missverständnisse zu vermeiden, wurden den IT-Beauftragten im Gespräch alle Fragen genauer erklärt und mit Beispielen versehen. Einzelne Fragen wurden nur in Abhängigkeit anderer Fragen gestellt, welche mit "Ja" beantwortet wurden. So wurde beispielsweise die Frage "In welchen Bereichen setzen Sie KI ein?" nur bei Unternehmen gestellt, welche die Frage "Setzen Sie in Ihrem Unternehmen künstliche Intelligenz ein?" mit "Ja" beantwortet haben. Insgesamt wurde im Zeitraum von Juni 2023 bis März 2024 mit 20 verschiedenen Unternehmen ein Cybersecurity-Checkup durchgeführt. Die Größe der teilnehmenden Unternehmen lässt sich wie folgt aufschlüsseln[1]:

- Kleinstunternehmen: 9
- Kleine Unternehmen: 3
- Mittlere Unternehmen: 8

[1] https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/_inhalt.html

2 Aufbereitete Erkenntnisse aus den Cybersecurity-Checkups

In diesem Kapitel stellen wir die Fragen vor, die wir den Unternehmen gestellt haben und präsentieren deren Ergebnisse. Zusätzlich führen wir den unseres Erachtens Soll-Zustand bei dieser Frage/Thematik an.

`Haben Sie einen Informationssicherheitsbeauftragten?`

Der oder die Informationssicherheitsbeauftragte ist die zentrale Kontaktperson für alle Fragen, die die Informationssicherheit im Unternehmen betreffen. Die Vergabe dieser Rolle soll helfen Zuständigkeiten zu klären, damit sicherheitsrelevante Aufgaben im Tagesgeschäft nicht zurückfallen. Zieht man den BSI-Standard 200-2 zu Rate, gehören zu den Aufgaben dieser Person das Steuern und Koordinieren des Sicherheitsprozesses, die Mithilfe bei der Erstellung einer Sicherheitsleitlinie, die Koordination der Erstellung eines Sicherheitskonzepts, das Anfertigen von Realisierungsplänen für Sicherheitsmaßnahmen sowie die Initiierung und Überprüfung derer Umsetzung, das Berichten über den Status der Informationssicherheit an die Leitungsebene, das Koordinieren sicherheitsrelevanter Projekte, das Untersuchen sicherheitsrelevanter Vorfälle und das Abhalten von Schulungen für Mitarbeitende sowie deren Sensibilisierung für die Informationssicherheit des Unternehmens [1]. Idealerweise ist die Person selbst nicht Teil der IT-Abteilung, um Interessenskonflikte zu vermeiden und die Unabhängigkeit zu wahren. Der oder die Informationssicherheitsbeauftragte vereint Fachexpertise und organisatorisches Talent, und ist mit den Geschäftsprozessen des Unternehmens vertraut.

Diese Frage wurde von 25% mit Ja und 75% mit Nein beantwortet.

`Haben Sie einen Datenschutzbeauftragten?`

Unternehmen müssen die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten jederzeit nachweisen können [2]. Ferner sind sie dazu verpflichtet, ein Verzeichnis über ihre Verarbeitungstätigkeiten von personenbezogenen Daten zu führen [3]. Zudem müssen sie unter bestimmten Voraussetzungen eine*n Datenschutzbeauftragte*n benennen [4,5].

Diese Frage wurde von 45% der Unternehmen mit "Ja" beantwortet.

`Ist Ihr Unternehmen nach ISO/IEC 27001 zertifiziert?`

Der ISO-Standard 27001 betrifft den Betrieb eines Informationssicherheitsmanagementsystems (ISMS), das Unternehmen dabei unterstützt, mit Sicherheitsrisiken angemessen umzugehen. Das ISMS legt dabei die Methoden und Instrumente fest, mit denen die die Informationssicherheit betreffenden Aktivitäten gelenkt werden sollen [6]. Der Standard umfasst Kriterien für den Aufbau, die Einführung, den Betrieb, die Überwachung und die kontinuierliche Verbesserung eines solchen Managementsystems [7]. Weiterhin kann die Zertifizierung nach diesem Standard auch als Vertrauensnachweis gegenüber Kunden angewendet werden.

Hier war die Antwort nur in 3 Fällen (15%) "Ja".

Ist Ihr Unternehmen nach BSI Grundschutz zertifiziert?

Neben der Möglichkeit des Aufbaus eines ISMS nach ISO/IEC 27001 können sich Unternehmen auch nach dem IT-Grundschutz des BSI zertifizieren lassen. Der IT-Grundschutz verfolgt einen ganzheitlichen Ansatz: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet [8]. Dabei liefern die BSI-Standards bewährte Vorgehensweisen und das IT-Grundschutz-Kompendium konkrete Anforderungen.

Nach eigener Aussage war kein einziges Unternehmen nach BSI Grundschutz zertifiziert.

Nutzen Sie eine Methode zur Bedrohungsanalyse?

Eine Bedrohungsanalyse hilft dabei, Bedrohungen für Systeme systematisch zu identifizieren, um deren Auswirkungen einschätzen und bewerten zu können. Sie ist somit ein organisatorisches Hilfsmittel, um die Informationssicherheit im Unternehmen zu stärken. Die Bedrohungsanalyse umfasst das Identifizieren zu schützender Komponenten sowie das Identifizieren, Dokumentieren und Bewerten von Bedrohungen [9].

Eine Bedrohungsanalyse kam in 40% der Fälle zum Einsatz.

Gibt es einen Notfallplan mit definierten Prozessen und Aufgaben im Falle eines Cyberangriffs?

Ein wichtiger Punkt des Notfallmanagements ist das Vorhandensein von Notfallplänen mit definierten Prozessen und Aufgaben für den Ernstfall. Existieren keine Pläne, muss bei Auftreten eines Sicherheitsvorfalls spontan überlegt werden, was als nächstes zu tun ist. Notfallpläne helfen dabei möglichst schnell und angemessen auf Bedrohungen zu reagieren. Für das Verhalten im Ernstfall existiert ein Maßnahmenkatalog zum Notfallmanagement mit Fokus auf IT-Notfälle des BSI [10]. Darin wird zur Erstellung folgender Produkte durch den Notfallbeauftragten geraten: Einer Leitlinie zum Notfallmanagement, eines Notfallvorsorgekonzepts und eines Notfallhandbuchs. Das Notfallhandbuch sollte Geschäftsfortführungs- und Wiederanlaufpläne umfassen. Zusätzlich können in diesem Handbuch auch Pläne für Sofortmaßnahmen, ein Krisenstabsleitfaden und ein Krisenkommunikationsplan hinterlegt werden [11]. Das BSI empfiehlt zudem den Einsatz von IT-Notfallkarten [12]. Auf diesen wird das richtige Verhalten bei IT-Notfällen geschildert, das drei wesentliche Punkte abdecken sollte: Die Kenntnis der Ansprechpartner für IT-Notfälle in der Organisation und deren Erreichbarkeit, die sofortige Weitergabe entscheidender Informationen und der Hinweis, dass Gegenmaßnahmen nur nach Absprache oder auf Anweisung der Ansprechpartner erfolgen soll.

26% der Unternehmen hatten derartige Pläne vorbereitet.

Wurden Sie schon einmal Opfer einer Cyberattacke?

Die Frage nach einem bereits früher erfolgten Sicherheitsvorfall dient dazu die Bewertung der umgesetzten Maßnahmen bei dem befragten Unternehmen besser einschätzen zu können. Gab es in der Vergangenheit bereits Vorfälle, bei welchen Daten gestohlen oder gelöscht wurden, es aber beispielsweise weiterhin keine ausreichende Backup-Strategie gibt, kann man daraus schließen, dass die Unternehmen bei den erforderlichen Maßnahmen mehr Unterstützungsbedarf benötigen.

Jedes dritte der befragten Unternehmen wurde in der Vergangenheit angegriffen.

`Haben Ihre Mitarbeitenden schon einmal eine IT-Sicherheitsschulung erhalten?`

Häufige Ziele von Angreifenden stellen oftmals nicht direkt die technischen Systeme, sondern die Mitarbeitenden des Unternehmens dar. Durch *Social Engineer*ing und *Phishing-Attacken* versuchen Angreifende die Mitarbeitenden zur Herausgabe von vertraulichen Informationen oder zur Durchführung schädlicher Aktionen zu motivieren. Diese Angriffe können erschwert werden, wenn sich alle Mitarbeitenden dieser Gefahren bewusst sind und diese auch erkennen können. Dieses Bewusstsein sollte regelmäßig in IT-Sicherheitsschulungen gestärkt werden, insbesondere bei Mitarbeitenden, welche regelmäßig mit externen Personen kommunizieren [13].

Bei dieser Frage stimmten 35% für "Ja" und 65% für "Nein".

`Hat jeder Mitarbeiter ein eigenes Benutzerkonto (oder teilen sie sich ein gemeinsames Konto)?`

Alle Mitarbeitenden in einem Unternehmen mit Zugriff auf IT-Systeme sollten eigene Benutzerkonten für diese Systeme erhalten, und es sollten möglichst keine Konten existieren, welche von mehreren Mitarbeitenden gemeinsam genutzt werden (*Account Sharing*) [14]. Dadurch können IT-Sicherheitsvorfälle besser nachvollzogen und bekämpft werden, sobald ermittelt wurde, welches Konto als Einfallstor ins Unternehmensnetzwerk diente. Bei personenbezogenen Benutzerkonten kann der jeweilige Mitarbeiter bzw. die jeweilige Mitarbeiterin gezielter nach ungewöhnlichen Ereignissen in den letzten Tagen befragt werden, was bei einem geteilten Konto von mehreren Mitarbeitenden nur schwer möglich ist.

Jedes einzelne Unternehmen gab an, dass ihre Mitarbeitenden über ein eigenes Benutzerkonto verfügen.

`Dürfen Ihre Mitarbeiter nur auf für sie relevante Daten und Dienste zugreifen (oder hat jeder Zugriff auf alles)?`

Berechtigungen sollten so vergeben werden, wie es für die Erfüllung der vorgesehenen Aufgaben notwendig ist (*Need-to-know-Prinzip*). Außerdem sollte die Vergabe von Rechten möglichst restriktiv geschehen (*Principle of Least Privilege*) [15]. Dies reduziert zum einen das Risiko des versehentlichen Löschens von Daten, andererseits können Angreifende so ebenfalls nur auf eine Teilmenge der gesamten Unternehmensdaten zugreifen, wenn ein Konto eines Mitarbeitenden kompromittiert wurde.

Zwei Drittel (68%) haben angegeben, dass die Mitarbeitenden nur auf für sie relevante Daten zugreifen dürfen.

`Setzen Sie Zwei-Faktor-Authentisierung ein?`

Bei besonders schützenswerten Systemen und Diensten sollte eine Zwei-Faktor-Authentisierung eingesetzt werden [16]. Der zweite Faktor soll das Konto zusätzlich schützen, auch wenn das verwendete Passwort Angreifenden bereits bekannt ist. Dieser Faktor kann beispielsweise ein Code per SMS, eine Anwendung auf einem Smartphone, ein persönliches Merkmal wie ein Fingerabdruck oder Gesichtszüge, oder ein von einem Hardware Token generiertes Einmalkennwort sein. Die Art des zweiten Faktors die sich für den jeweiligen Einsatzzweck am besten eignet, ist situationsabhängig, die Vor- und Nachteile sowie Kosten und Nutzen sollten vorab im Unternehmen diskutiert werden. Wichtig ist, dass die beiden Faktoren nicht auf einem Gerät zusammenlaufen, und es am Ende effektiv wieder nur einen Faktor gibt, der geschützt werden muss. Wird beispielsweise Online-Banking hauptsächlich über ein Smartphone durchgeführt und der zweite Faktor besteht aus einer SMS an eben dieses, dann kontrolliert ein Angreifender direkt beide Faktoren, sobald das

Smartphone kompromittiert wurde. Zwei-Faktor-Authentisierung sollte bewusst an besonders relevanten Stellen eingesetzt werden, da der entstehende Mehraufwand die Benutzer auf Dauer einschränken kann, und diese dann ggf. Wege zur Umgehung der Richtline etablieren, wodurch die IT-Sicherheit insgesamt verringert anstatt erhöht wird.

65% gaben an, Zwei-Faktor-Authentisierung einzusetzen.

Gibt es eine Passwortrichtlinie?

Grundsätzlich sollten alle eingesetzten Kennwörter hinreichend lang und komplex sein [17]. Für jeden Dienst sollte zudem ein individuelles Kennwort vergeben werden. Dies verhindert *Credential Stuffing*, bei dem erbeutete Anmeldedaten eines Dienstes über mehrere, nicht direkt damit in Beziehung stehende andere Dienste ausprobiert werden, um auch diese Konten zu infiltrieren. Um ein Aufschreiben der Passwörter auf Papier zu verhindern, wir der Einsatz eines Passwortmanagers unter Verwendung eines starken Master-Passworts empfohlen. Mitarbeitende sollten selbst unter Kollegen niemals eines ihrer Passwörter teilen, und dieses sofort ändern, falls eine andere Person davon Kenntnis erlangt.

Bei vier von fünf Unternehmen (80%) gab es eine Passwortrichtlinie.

Wird die Passwortrichtlinie technisch forciert?

Damit die Mitarbeitenden auch tatsächlich ein sicheres Kennwort wählen, sollte technisch eine Mindestkomplexität der Kennwörter erzwungen werden. Schwache Kennwörter sollten direkt abgelehnt werden.

Bei den 16 Unternehmen, die eine Passwortrichtlinie hatten, wurde diese in 69% der Fälle technisch durchgesetzt.

Gibt es Richtlinien zur physischen Sicherheit?

Grundsätzlich sollte darauf geachtet werden, beim Verlassen des Arbeitsplatzes stets das Arbeitsgerät zu sperren, um unbefugte Zugriffe zu verhindern, auch wenn es sich nur um eine (vermutlich) kurze Abwesenheit handeln wird [13]. Zusätzlich können Systeme nach längerer Inaktivität automatisch gesperrt werden, falls Mitarbeitende einmal das Sperren vergessen sollten. Büroräume sollten stets abgeschlossen werden, sobald der letzte Mitarbeitende den Raum verlässt. Um potenziellen Angreifenden den Zugang zum Gebäude zu erschweren, sollte bei fremden Personen auf das klassische Türaufhalten verzichtet, oder zumindest freundlich nach ihrem Anliegen gefragt werden. Kunden und Besucher sollten sich außerdem nicht unbeaufsichtigt in Arbeitsräumen aufhalten. An den Arbeitsplätzen ist darauf zu achten, dass keine sensiblen Informationen offen herumliegen, wenn die Gefahr besteht, dass fremde Personen Zugang zu den Büros erhalten können.

65% der Unternehmen stimmten bei dieser Frage für "Ja".

`Zu welchen Bereichen haben Kunden und Besucher Zugang? Sind sie je unbeaufsichtigt?`

Kunden und Besucher sollten sich nicht unbeaufsichtigt in Arbeitsräumen aufhalten. An den Arbeitsplätzen ist darauf zu achten, dass keine sensiblen Informationen offen einsehbar sind, wenn die Gefahr besteht, dass fremde Personen Zugang zu den Büros erhalten können.

Da es sich um eine Freitextfrage handelt, werden hier keine Prozentzahlen aufgeführt.

`Welche Betriebssysteme setzen Sie ein?`

Als Softwaregrundlage müssen die eingesetzten Betriebssysteme selbst gut geschützt sein. Dazu müssen sie regelmäßig mit Sicherheitsupdates versehen und sicher konfiguriert werden [18]. Alte Software und veraltete Treiber, die nicht mehr verwendet werden, sollten vom Betriebssystem entfernt werden, um Angreifenden kein Einfallstor zu bieten. Fernzugänge sollten gut geschützt oder entfernt werden, falls diese nicht benötigt werden.

Da es sich um eine Freitextfrage handelt, werden hier keine Prozentzahlen aufgeführt.

`Welche Antivirensoftware setzen Sie ein?`

Aus Gründen der Wettbewerbsverzerrung können wir keine konkreten Produkte empfehlen oder bewerten. Wichtig ist, dass sich die Verantwortlichen Unternehmen Gedanken zu verschiedenen Antivirenprogrammen machen, deren Vor- und Nachteile sowie Kosten abschätzen und sich bewusst für ein Produkt entscheiden.

Da es sich um eine Freitextfrage handelt, werden hier keine Prozentzahlen aufgeführt.

`Welche Firewalls setzen Sie ein?`

Ein Whitelisting-Ansatz des gewünschten Netzwerkverkehrs ist aufwändiger als ein Blacklisting von unerwünschten Paketen, erhöht die Sicherheit jedoch signifikant. Sofern nur genau spezifizierter Internet-Verkehr am Arbeitsplatz erforderlich ist, sollte das Unternehmen zunächst allen Netzwerkverkehr blockieren und nach und nach Kommunikation erlauben, wo immer sie benötigt wird [19]. Dazu sollten alle Firewall-Regeln regelmäßig überprüft und angepasst werden. So können auch alte Regeln gelöscht werden, wenn sie nicht mehr benötigt werden, um die Übersicht und Leistungsfähigkeit zu erhöhen. Da Firewalls selbst ein Ziel für Angreifende darstellen können, muss regelmäßig überprüft werden, ob neue Sicherheitsupdates des Herstellers vorliegen und diese installiert werden. Der Zugang zur Firewall muss ebenfalls gut geschützt werden, daher sollten Standardzugangsdaten geändert und mit sicheren Kennwörtern versehen werden. Außerdem sollten nur ausgewählte Mitarbeitende Zugriff auf die Konfiguration der Firewall erhalten. Dadurch wird der Zugriff durch Angreifende erschwert, welche sonst einzelne Firewall-Regeln deaktivieren und sich leichter im Netzwerk ausbreiten können. Auch hier können wir keine konkreten Produkte empfehlen und raten den Unternehmen dazu, sich ausgiebig über die verschiedenen Anbieter zu informieren.

Da es sich um eine Freitextfrage handelt, werden hier keine Prozentzahlen aufgeführt.

`Ist das Netzwerk segmentiert (oder hängen alle Geräte in einem großen Netzwerk zusammen)?`

Bei einem größeren Netzwerk ist es ratsam, dieses in einzelne, kleinere Netzwerke zu unterteilen und diese entsprechend voneinander zu trennen [20]. Dies erschwert die Ausbreitung von Angreifenden, die bereits eine Maschine im Netzwerk infiltriert haben, und hilft dabei die Angriffsfläche zu reduzieren. Wird ein Angriff erkannt, können betroffene Teilnetze isoliert werden, ohne die anderen zu beeinflussen.

Etwa die Hälfte (47%) gab an, dass das Netzwerk segmentiert sei.

`Gibt es einen Netzwerkplan, bei dem sauber dokumentiert ist, welche Maschinen existieren, wer mit wem kommuniziert und welche Ports geöffnet sind?`

In einem Netzwerkplan wird die gesamte Unternehmensinfrastruktur dokumentiert [20]. Der Plan gibt eine Übersicht aller im Netzwerk befindlichen Geräte wieder. Idealerweise wird auch ersichtlich, welche Geräte untereinander kommunizieren und welche Ports geöffnet sind. Bei einem Angriff gibt der Plan eine schnelle Übersicht über mögliche Einfallstore, potenziell infizierte Systeme und nächste Ziele. So können schnell relevante Netzwerke isoliert oder Ports geschlossen werden. Zusätzlich wird die Wahrscheinlichkeit gemindert, dass einzelne Systeme während der Isolierung oder Neuinstallation übersehen werden. Wird ein derartiger Plan erst nach dem Erkennen des Angriffs angefertigt, verstreicht wertvolle Zeit, die den Angreifenden in die Hände spielt.

Bei 42% existierte ein derartiger Netzwerkplan.

`Wird die Infrastruktur überwacht?`

Um aktive Angreifende zu entdecken, bevor diese Schaden anrichten, ist es ratsam, das Netzwerk und die IT-Systeme zu überwachen [21]. So kann Alarm geschlagen werden, wenn mehrfach falsche Kennworteingaben getätigt werden oder ungewöhnlich viel Netzwerkverkehr stattfindet. Beide Ereignisse können auf einen aktiven Angreifer hindeuten, welcher versucht in das System einzudringen oder Daten zu exfiltrieren. Darüber hinaus können unbenutzte Ports der verschiedenen Dienste überwacht werden. Sollte einer oder mehrere dieser Ports angesprochen werden, könnte dies auf einen Portscan hinweisen, bei dem Angreifende versuchen mehr Informationen über das System zu sammeln. Auf den Systemen selbst können ungewöhnliche Anmeldezeiten der Mitarbeitenden (beispielsweise nachts) oder die Erzeugung von Dateien an ungewöhnlichen Pfaden überwacht werden. Die Gesamtheit dieser Maßnahmen werden unter dem Begriff der *Intrusion Detection* zusammengefasst und erlauben es einem Unternehmen schnell zu handeln, wenn ein Angreifer im System entdeckt wird.

Bei etwa der Hälfte (53%) kam ein Monitoring zum Einsatz.

`Nutzen Sie Cloud-Lösungen von Drittanbietern?`

Speichern Unternehmen Daten in der Cloud oder nutzen allgemein Cloud-Dienste, geben sie einen Teil ihrer Verantwortung an den Cloud-Dienstleister ab [22]. Dieser muss sicherstellen, dass die Daten verfügbar und unverfälscht sind und dass diese nicht in die falschen Hände gelangen. Da dies zum Kerngeschäft der Cloud-Dienstleister gehört, können sie diese Kriterien potenziell besser gewährleisten als das Unternehmen selbst, insbesondere bei kleinen Unternehmen mit wenig Infrastruktur. Geklärt werden muss jedoch, ob sich datenschutzrechtliche Probleme ergeben, welche ggf. durch ein Verschlüsseln der Daten gelöst werden

können. Die Verantwortlichen müssen sich überlegen, ob die nötige Kompetenz und der Sachverstand im Unternehmen vorhanden sind, um eigenständig Cloud-Dienste zu betreiben und dort Daten zu speichern. Ist dies nicht der Fall, kann sich über existierende Cloud-Anbieter informiert und recherchiert werden, wie vertraulich und zuverlässig diese sind.

Externe Cloud-Lösungen erfreuten sich großer Beliebtheit (82% der Unternehmen).

Machen Sie regelmäßig Backups Ihrer Daten?

Um Datenverlust zu vermeiden, müssen regelmäßig Sicherheitskopien aller wichtigen Systeme angefertigt werden [23]. Das Intervall und die Aufbewahrungsdauer hängen dabei von der Wichtigkeit des jeweiligen Systems ab. Die Qualität der Sicherheitskopien lässt sich in drei Schutzstufen einteilen, welche vor bestimmen Situationen schützen.

1. *Einfacher Defekt*: Sollte ein einzelnes System ausfallen oder gestohlen werden, so können die Daten mit einer einfachen Sicherheitskopie wiederhergestellt werden.
2. *Brand oder Wasserschaden*: Bei einem Brand oder großflächigen Wasserschaden im Serverraum eines Unternehmens können die Sicherheitskopien ebenfalls vernichtet werden. In diesem Fall würden kritische Unternehmensdaten trotz täglicher Datensicherung und langer Aufbewahrungsdauer verloren gehen. Bei kleinen Unternehmen, die die Sicherheitskopien nur auf einer externen Festplatte speichern, könnten bei einem Diebstahl sowohl Server als auch externe Festplatte gestohlen werden, was zum gleichen Ergebnis führt. Um diese Situationen zu verhindern, sollten Sicherheitskopien zusätzlich an einem weiteren Ort gelagert werden, sei es bei einem Cloud-Anbieter, einer Außenstelle des Unternehmens oder gar zuhause bei der Geschäftsführung.
3. *Aktive Angreifende*: Haben Angreifende Zugriff auf das Firmennetzwerk erhalten, so besteht die Gefahr, dass sie neben eingesetzten Servern auch auf die Infrastruktur der Datensicherung stoßen und zugreifen. Wenn es den Angreifenden möglich ist die Daten der Sicherheitskopien zu löschen oder zu überschreiben, dann schützen auch extern gespeicherte Sicherheitskopien nicht vor Datenverlust. Um gegen aktive Angriffe zu schützen, müssen die Sicherheitskopien entweder physisch vom Netzwerk getrennt sein oder sie dürfen technisch nicht überschrieben bzw. gelöscht werden können, sobald sie einmal angelegt wurden.

Neun von zehn Unternehmen gaben an, regelmäßig Sicherheitskopien anzulegen.

Können die Backups von einem Angreifer überschrieben werden?

Um vor Verschlüsselungstrojanern und anderen aktiven Angreifenden geschützt zu sein, müssen die Sicherheitskopien auch die dritte der oben genannten Stufen erfüllen.

Vor Angreifern geschützt war nur die Hälfte (53%) der Sicherheitskopien.

Setzen Sie alte Software ein, die keine Sicherheitsupdates mehr erhält?

Eines der Haupteinfallstore für Cyberangriffe stellt veraltete Software dar. Erhält eine Software vom Hersteller keine Sicherheitsupdates, so können sich über die Zeit hinweg mehr und mehr bekannte Sicherheitslücken ansammeln, und die Gefahr einer Remote-Codeausführung steigt. Daher muss bereits vor dem offiziellen Ende der Unterstützung des Programms (End of Life, EOL) nach einer Alternative für das Programm gesucht und der Wechsel durchgeführt werden [18]. Damit auf bei neuer Software keine Sicherheitslücken ausgenutzt werden können, muss regelmäßig überprüft werden, ob für diese Programme neue Sicherheitsupdates zur Verfügung stehen. Ist dies der Fall, sollten die Updates umgehend installiert werden [18].

Zwei Drittel (65%) der Befragten setzten nur aktuelle Software ein, bei 35% kam auch veraltete Software zum Einsatz.

`Wie oft überprüfen Sie ob neue Sicherheitsupdates existieren und spielen diese ein?`

Damit auf bei neuer Software keine Sicherheitslücken ausgenutzt werden können, muss regelmäßig überprüft werden, ob für diese Programme neue Sicherheitsupdates zur Verfügung stehen. Ist dies der Fall, sollten die Updates umgehend installiert werden [18].

Da es sich um eine Freitextfrage handelt, werden hier keine Prozentzahlen aufgeführt.

`Wurde Ihre Infrastruktur schon einmal einem Penetrationstest unterzogen?`

Bei einem Penetrationstest wird die Unternehmensinfrastruktur von Externen auf Sicherheitslücken untersucht. Die Penetrationstester schlüpfen dabei in die Rolle eines Angreifenden und versuchen in Absprache mit dem Unternehmen in verschiedene Systeme einzudringen, vertrauliche Daten zu stehlen und die Kontrolle über die Infrastruktur zu übernehmen [24]. Im Anschluss verfassen die Penetrationstester einen Bericht, in dem sie alle gefundenen Schwachstellen festhalten und dem Unternehmen kommunizieren, sodass sie geschlossen werden können, bevor sie echte Angreifende ausnutzen können. Penetrationstests sind somit eine gute Möglichkeit die Infrastruktur mit externer Expertise untersuchen zu lassen und Schwachstellen aufzudecken. Allerdings bedeutet ein erfolgloser Penetration Test nicht, dass das System sicher ist und über keine Schwachstellen verfügt. Zudem werden für einen aussagekräftigen den Test umfangreiche finanzielle und personelle Ressourcen benötigt. Daher halten wir einen Penetrationstest bei kleinen Unternehmen nur nach einer durchgeführten Risikobewertung und einer entsprechenden Bedrohungslage für sinnvoll. Andernfalls sollten die Ressourcen in die Behebung bekannter Probleme investiert werden, anstatt noch zusätzliche Probleme aufzudecken, welche dann ebenfalls erst noch behoben werden müssen.

Ein Viertel (26%) der befragten Unternehmen hat in der Vergangenheit einen Penetrationstest durchführen lassen.

`Haben Sie eine security.txt auf Ihren Webseiten platziert?`

Oftmals entdecken Sicherheitsforscher eine Sicherheitslücke in einer Webanwendung, finden dann jedoch keinen passenden Ansprechpartner, um die Sicherheitslücke zu melden. Sie wenden sich an eine generische info@-Adresse im Impressum, woraufhin die Nachricht je nach Leser womöglich ignoriert oder als Spam eingestuft wird. Um dies zu verhindern, kann mit wenig Aufwand eine security.txt[2] Datei erstellt werden, welche eine Kontaktadresse für Sicherheitslücken enthält. In ihrer einfachsten Ausführung hat die security.txt das folgende Format:

```
Contact: mailto:security@example.com
Expires: 2020-01-01T23:00:00.000Z
```

Die Datei wird unter https://example.com/.well-known/security.txt abgelegt.

Die Neuartigkeit der security.txt hat sich in den Antworten widergespiegelt. Die meisten Befragten kannten dieses Konzept nicht, nur 6% hatten bereits eine derartige Datei auf ihrem Webserver hinterlegt.

[2] https://securitytxt.org/

Setzen Sie IoT-Geräte ein?

Das Internet of Things bezeichnet die Vernetzung einer Vielzahl von physischen Geräten, die mittels Sensoren ihre Umgebung erfassen und durch den Einsatz von Aktuatoren diese wiederum beeinflussen. Durch den Einsatz vielfältiger Kommunikationsschnittstellen wie NFC, Bluetooth und WLAN werden kontinuierlich Daten erfasst, ausgetauscht und verarbeitet. Die Fähigkeit solcher Systeme mit einer Vielzahl an Parametern umgehen zu können hat dazu geführt, dass sie auch in industriellen Fertigungsanlagen Verwendung finden. IoT-Geräte sind grundsätzlich ein beliebtes Ziel für Angreifende, da sie durch ihre Anbindung an das Internet oftmals von extern erreichbar sind, bekannte Sicherheitslücken aufweisen und bei Unternehmen nicht im Netzstrukturplan aufgeführt werden. Erlangen Angreifende die Kontrolle über ein derartiges IoT-Gerät, kommen sie der Kontrolle der relevanten Infrastruktur im Unternehmen einen Schritt näher. Um dies zu verhindern, können IoT-Geräte an ein isoliertes Netzwerk angeschlossen werden. Zudem sollten die IoT-Geräte beobachtet und regelmäßig aktualisiert werden, damit sie nicht zur Ausbreitung im Netzwerk verwendet werden können. Falls Mitarbeitende eigene Geräte im Unternehmenskontext einsetzen dürfen, sollte von der IT vorgeschrieben werden, diese Geräte nur mit einem dafür vorgesehenen Netz ("Private Devices") zu verbinden, um den Zugriff auf andere Dienste und Geräte einzuschränken.

IoT-Geräte fanden bei zwei Dritteln (63%) Einzug.

Setzen Sie in Ihrem Unternehmen künstliche Intelligenz ein?

Künstliche Intelligenz (KI) kann unter anderem zur Bilderkennung, Analyse großer Datenmengen oder Automatisierung und Entscheidungsfindung eingesetzt werden. KI wird jedoch auch eingesetzt, um Cyberangriffe durchzuführen oder diese zu erkennen und abzuwehren. Schließlich können auch KI-Systeme selbst von Angreifenden ins Visier genommen werden, um die von der KI getroffenen Entscheidungen zugunsten der Angreifenden zu manipulieren.

Künstliche Intelligenz kam bei 30% der Unternehmen zum Einsatz.

In welchen Bereichen setzen Sie KI ein?

Unterschiedliche Domänen besitzen unterschiedliche Randbedingungen, die eingehalten werden müssen. Diese können rechtlicher Natur sein (regulatorischer Rahmen, Safety-Anforderungen, Echtzeitbedingungen, ...). Dadurch eignen sich manche Einsatzgebiete eher für den Einsatz künstlicher Intelligenz als andere. Gerade in Domänen, die mit hohen Risiken verbunden sind, ist es wichtig den Einsatz von KI zu hinterfragen und Maßnahmen vorzubereiten, die ein Fehlverhalten verhindern oder zumindest einschränken können.

Da es sich um eine Freitextfrage handelt, werden hier keine Prozentzahlen aufgeführt.

Wurde die KI selbst entwickelt (oder eingekauft)?

Die Frage, ob die künstliche Intelligenz selbst entwickelt oder eingekauft wurde, hat den Hintergrund, dass herausgefunden werden sollte, ob bei Eigenentwicklungen wichtige Aspekte der Cybersicherheit mitbedacht werden. Vorteile einer Eigenentwicklung sind mehr Transparenz und Nachvollziehbarkeit der Ausgaben, sowie die Hoheit über die (Trainings-)daten. Nachteile können sein, dass etwa Angriffe wie Adversarial Learning nicht bei der Absicherung mitbetrachtet wurden.

Selbst entwickelt wurde die KI bei 33%, in 67% der Fälle wurde sie von externen Anbietern eingekauft.

`Führt die KI selbstständig folgenreiche Aktionen aus (oder hat stets ein Mensch das letzte Wort)?`

Den Ausgaben einer KI sollte nicht blind vertraut werden. Fehler in den Trainingsdaten können dazu führen, dass Entscheidungen getroffen werden, die, je nach Einsatzzweck, weitreichende Folgen haben könnten. So können Fehlentscheidungen einer KI zu einem finanziellen Risiko, aber auch zur Gefahren für das Leib und Leben führen.

In 17% der Fälle führte die KI unüberwacht folgenreiche Aktionen aus.

`Setzen Sie in Ihrem Unternehmen eine Blockchain ein?`

Seit Einführung der Blockchain sehen Unternehmen aus verschiedensten Bereichen einen Vorteil beim Einsatz einer Blockchain anstelle einer traditionellen, verteilten Datenbank. Aufgrund der Neuheit des Konzepts werden die Sicherheitseigenschaften und -garantien einer Blockchain jedoch häufig missverstanden, wodurch kein Sicherheitsgewinn entsteht.

Kein einziges Unternehmen setzte eine Blockchain ein, daher haben wir die folgenden beiden, vorgesehen Fragen nicht gestellt:

- In welchen Bereichen setzen Sie eine Blockchain ein?
- Warum haben Sie sich in diesem Fall für eine Blockchain entschieden?

`Haben Sie schon von Quantencomputern und deren Gefahren für die Kryptographie gehört?`

Eine große Gefahr stellen Quantencomputer für die asymmetrische Kryptographie dar, da durch Quantencomputer möglicherweise effizient Primzahlen faktorisiert und somit verbreitete Verfahren wie das RSA-Kryptosystem gebrochen werden können. Auf diese Art können Angreifende Chiffrate entschlüsseln, welche heute noch als sicher verschlüsselt gelten.

90% der befragten Unternehmen wussten bereits von den Gefahren von Quantencomputern.

`Haben Sie sich bereits Gedanken gemacht, wie Quantencomputer Ihr Unternehmen beeinflussen wird?`

Die Gefahren von Quantencomputern für die Kryptographie sollten in KMU nicht mit höchster Priorität betrachtet werden, da bislang nicht zu erwarten ist, dass Kryptosysteme zeitnah durch Quantencomputer gebrochen werden können. Dennoch sollte die Thematik im Unternehmen diskutiert werden, um deren Auswirkungen auf das eigene Unternehmen besser abschätzen zu können. Insbesondere falls das Unternehmen über verschlüsselte Geschäftsgeheimnisse o.ä. verfügt, bei denen ein heutiger Diebstahl mit zukünftiger Entschlüsselung einen nennenswerten Schaden für das Unternehmen bedeuten würde.

Die Hälfte der Unternehmen hat sich bezüglich Quantencomputern Gedanken zu ihrem Unternehmen gemacht.

3 Subjektive Erkenntnisse aus den Cybersecurity-Checkups

In diesem Kapitel stellen wir subjektive Erkenntnisse aus den Cybersecurity-Checkups vor.

Tabelle 2 im Anhang zeigt das Minimum, Maximum, den Durchschnitt und die Standardabweichung unserer Einschätzung, wie viel Verbesserungspotenzial bei den Unternehmen in Bezug auf die Frage existiert, absteigend sortiert nach der Einschätzung.

Bei unserer Einschätzung bedeutet eine Frage, die mit "Nein" beantwortet wurde nicht zwangsläufig, dass wir dort viel Verbesserungspotenzial sehen. Beispielsweise kann bei einem sehr kleinen Unternehmensnetzwerk eine Segmentierung des Netzwerks unnötig sein.

Bei den Fragen, welche Antivirensoftware und Firewall eingesetzt wird, beschränkte sich unsere Bewertung darauf, ob sich das Unternehmen hinreichend Gedanken zu diesem Thema gemacht und auf dieser Basis eine Entscheidung getroffen hat. Wir bewerten nicht die Effektivität verschiedener Antiviren- und Firewall-Lösungen und deren Anbieter.

Die drei Fragen, bei denen wir am wenigsten Verbesserungspotenzial sehen, sind "Welche Antivirensoftware setzen Sie ein?" (4,88), "Nutzen Sie Cloud-Lösungen von Drittanbietern?" (4,82) und "Zu welchen Bereichen haben Kunden und Besucher Zugang? Sind sie je unbeaufsichtigt?" (4,72). Bei der Frage nach der Antivirensoftware handelte es sich um eine Frage mit Freitextantwort, jedoch hatten sich alle Unternehmen Gedanken zu Antivirensoftware gemacht und sich für ein Produkt entschieden, wodurch wir an dieser Stelle wenig Verbesserungspotenzial gesehen haben. Bei den 82% der Unternehmen, die Cloudlösungen lokal verwalteten Dateien und Diensten vorziehen, hatten wir den Eindruck, dass dies aufgrund der Unternehmensgröße und eigenen Expertise das Mittel der Wahl ist und den übrigen 18% eine lokale Datenverarbeitung zuzutrauen war.

Externe Kunden und Besucher hatten nach Aussagen der Unternehmen nur in den seltensten Fällen Zugang zu schützenswerten Bereichen. Angriffe in Form einer Verkleidung als Paketbote o.ä. wären nur schwer möglich. Als Hauptgründe wurden dedizierte Besprechungsräume, keine Präsenztermine mit externen Partnern und ein kleines Kollegium, bei dem fremde Gesichter sofort auffallen würden, genannt. Die durchgängig hohe Bewertung spiegelt sich auch in der Standardabweichung wider. Die drei Fragen mit niedrigster Standardabweichung bei unserer Einschätzung sind "Welche Antivirensoftware setzen Sie ein?" (0,33), "Hat jeder Mitarbeiter ein eigenes Benutzerkonto (oder teilen sie sich ein gemeinsames Konto)?" (0,5) und "Nutzen Sie Cloud-Lösungen von Drittanbietern?" (0,53).

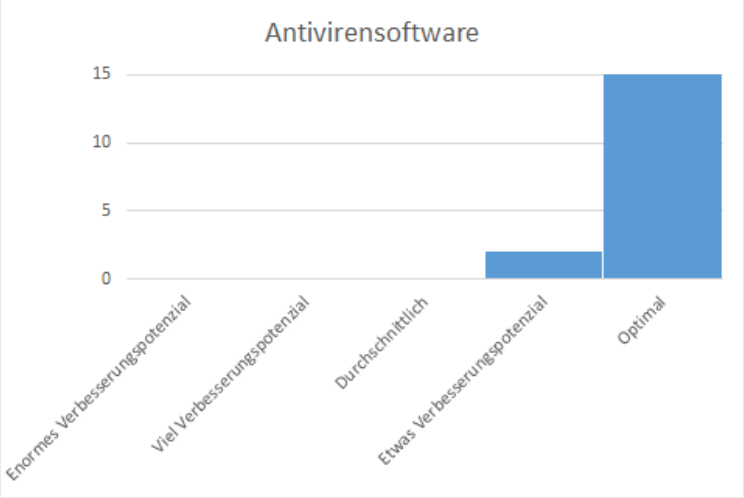

Abbildung 1: Antivirensoftware

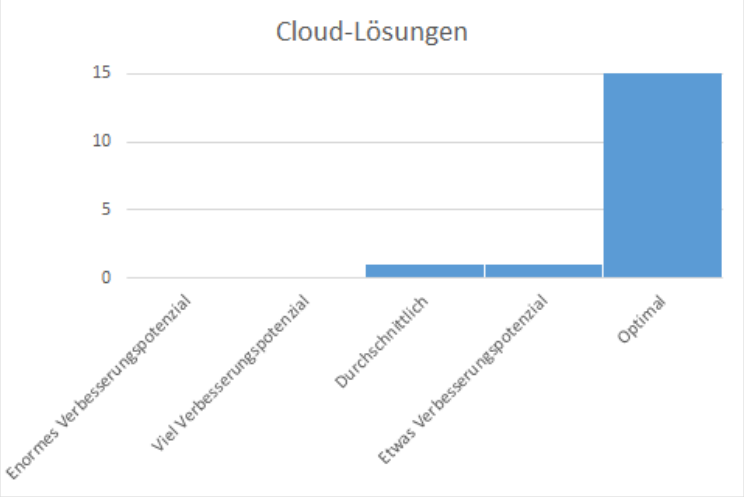

Abbildung 2: Cloud-Lösungen

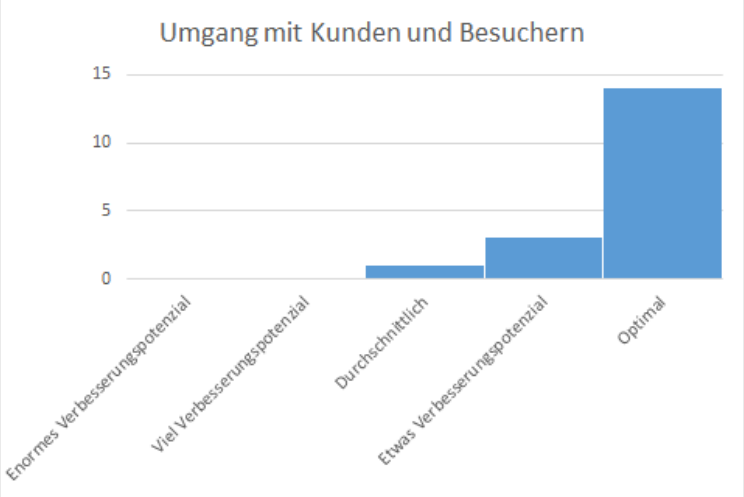

Abbildung 3: Umgang mit Kunden und Besuchern

Das meiste Verbesserungspotenzial sehen wir bei den Fragen "Gibt es einen Notfallplan mit definierten Prozessen und Aufgaben im Falle eines Cyberangriffs?" (2,95), "Nutzen Sie eine Methode zur Bedrohungsanalyse?" (3,30) und "Ist das Netzwerk segmentiert (oder hängen alle Geräte in einem großen Netzwerk zusammen)?" (3,68). Diesen Fragen wurden nur von einem Viertel bis Hälfte der Unternehmen mit "Ja" beantwortet, unser Eindruck war jedoch, dass beispielsweise ein Notfallplan auch in den anderen Unternehmen zumutbar wäre und einen deutlichen Mehrwert zur IT-Sicherheit beitragen würde.

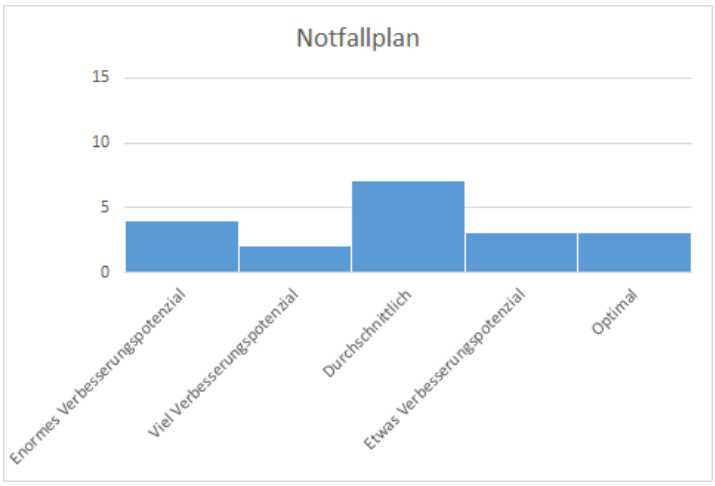

Abbildung 4: Notfallplan

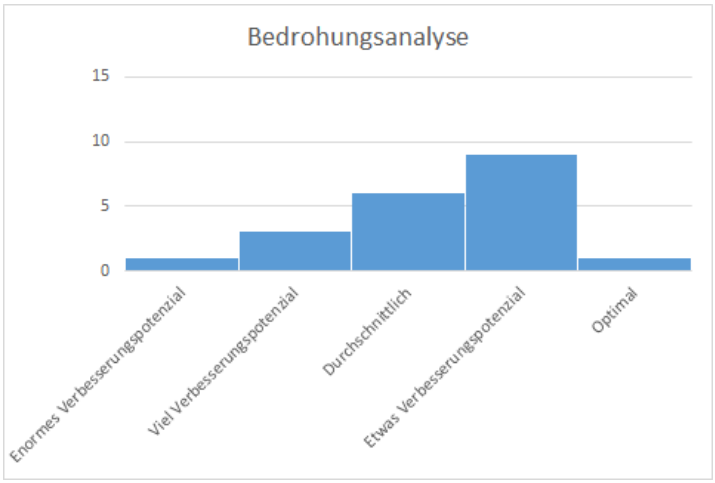

Abbildung 5: Bedrohungsanalyse

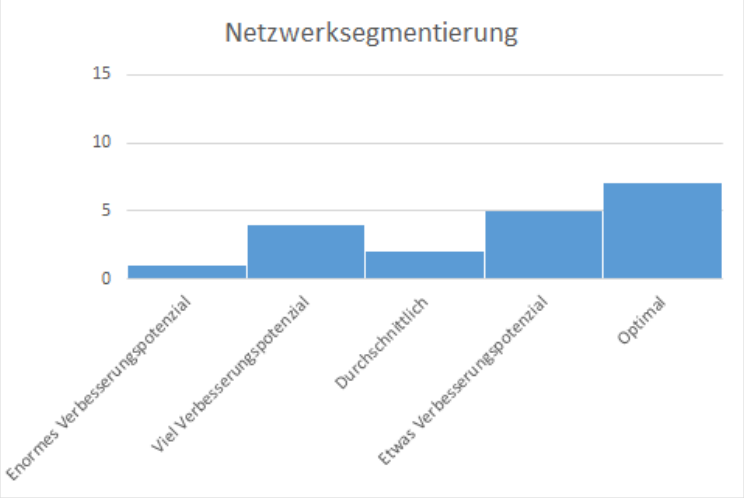

Abbildung 6: Netzwerksegmentierung

Die Fragen mit der höchsten Standardabweichung waren "Wird die Passwortrichtlinie technisch forciert?" (1,45), "Gibt es einen Notfallplan mit definierten Prozessen und Aufgaben im Falle eines Cyberangriffs?" (1,35) und "Ist das Netzwerk segmentiert (oder hängen alle Geräte in einem großen Netzwerk zusammen)?" (1,34). Bei diesen Fragen wurde ein "Nein" stark mit einem hohen Verbesserungspotenzial assoziiert, weil diese Maßnahmen unseres Erachtens bei fast allen Unternehmen zumutbar wären (während uns beispielsweise die Durchführung eines Penetrationstests nur bei wenigen Unternehmen sinnvoll erscheint).

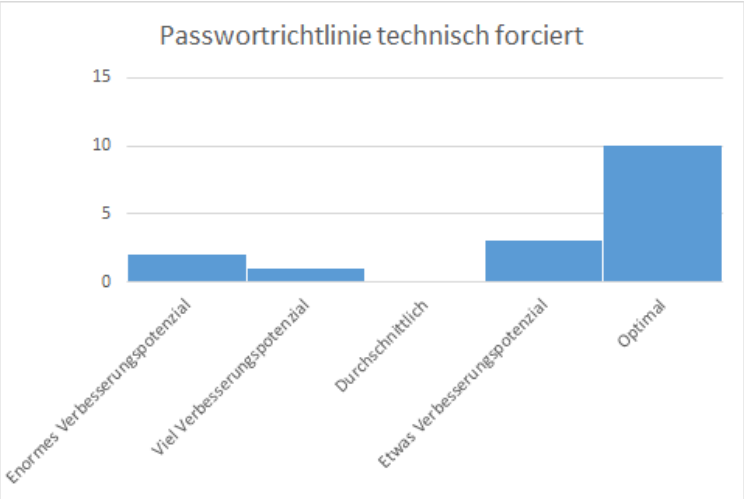

Abbildung 7: Passwortrichtlinie technisch forciert

4 Fazit

Die befragten Unternehmen waren bezüglich der umgesetzten Maßnahmen heterogen aufgestellt und somit unterschiedlich gut auf Cyberangriffe vorbereitet. Während die meisten technischen Sicherheitsmaßnahmen umgesetzt wurden, sahen wir die größten Missstände bei organisatorischen Maßnahmen wie Notfallplänen, Netzwerkplänen und Bedrohungsanalysen. Für Zertifizierung nach ISO/IEC 27001 oder BSI IT-Grundschutz hatten fast alle der Unternehmen aufgrund ihrer Größe keine Notwendigkeit gesehen.

Hinsichtlich innovativer Technologien wie Blockchain, KI und Quantencomputing waren die teilnehmenden Unternehmen eher zurückhaltend. Keines der Unternehmen setzte eine Blockchain ein, KI kam bei in 30% der Unternehmen zum Einsatz, wobei sich diese auf Bilderkennung und generative KI konzentrierte.

5 Literaturverzeichnis

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 Art. 5 Abs. 2

[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 Art. 30

[4] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 Art. 37

[5] https://www.gesetze-im-internet.de/bdsg_2018/ §38 Abs. 1

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html

[7] https://www.iso.org/standard/27001

[8] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

[9] https://www.plattform-i40.de/IP/Redaktion/DE/Standardartikel/Themen-und-Technologiekatalog/bedrohungsanalysen.html

[10] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog_node.html

[11] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/7_Notfaellebewaeltigen/4_Notfallhandbuch/Notfallhandbuch_node.html

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html

[13] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/IT-Sicherheit-am-Arbeitsplatz/it-sicherheit-am-arbeitsplatz_node.html

[14] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Basisschutz-fuer-Computer/Benutzerkonten/benutzerkonten_node.html

[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2022/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.html

[16] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

[17] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

[18] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Wichtige-Softwareupdates/wichtige-softwareupdates_node.html

[19] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Firewall/firewall_node.html

[20] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2021.pdf?__blob=publicationFile&v=2

[21] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134.pdf?__blob=publicationFile&v=1

[22] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/Cloud-Risiken-und-Sicherheitstipps/cloud-risiken-und-sicherheitstipps_node.html

[23] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.pdf?__blob=publicationFile&v=2

[24] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html

6 Anhang

Frage	Ja-Stimmen in Prozent	Stichproben-umfang
Hat jeder Mitarbeiter ein eigenes Benutzerkonto (oder teilen sie sich ein gemeinsames Konto)?	100	20
Haben Sie schon von Quantencomputern und deren Gefahren für die Kryptographie gehört?	90	20
Machen Sie regelmäßig Backups Ihrer Daten?	90	20
Nutzen Sie Cloud-Lösungen von Drittanbietern?	82	17
Gibt es eine Passwort-Richtlinie?	80	20
Wird die Passwortrichtlinie technisch forciert?	69	16
Dürfen Ihre Mitarbeiter nur auf für sie relevante Daten und Dienste zugreifen (oder hat jeder Zugriff auf alles)?	68	19
Setzen Sie Zwei-Faktor-Authentisierung ein?	65	20
Gibt es Richtlinien zur physischen Sicherheit?	65	20
Setzen Sie IoT-Geräte ein?	63	19
Wird die Infrastruktur überwacht?	53	19
Haben Sie sich bereits Gedanken gemacht, wie Quantencomputer Ihr Unternehmen beeinflussen wird?	50	18
Können die Backups von einem Angreifer überschrieben werden?	47	19
Ist das Netzwerk segmentiert (oder hängen alle Geräte in einem großen Netzwerk zusammen)?	47	19
Haben Sie einen Datenschutzbeauftragten?	45	20
Gibt es einen Netzwerkplan, bei dem sauber dokumentiert ist, welche Maschinen existieren, wer mit wem kommuniziert und welche Ports geöffnet sind?	42	19
Nutzen Sie eine Methode zur Bedrohungsanalyse	40	20
Haben Ihre Mitarbeitenden schon einmal eine IT-Sicherheitsschulung erhalten?	35	20
Setzen Sie alte Software ein, die keine Sicherheitsupdates mehr erhält?	35	20
Wurde die KI selbst entwickelt (oder eingekauft)?	33	6
Wurden Sie schon einmal Opfer einer Cyberattacke?	33	15

Setzen Sie in Ihrem Unternehmen künstliche Intelligenz ein?	30	20
Wurde Ihre Infrastruktur schon einmal einem Penetrationstest unterzogen?	26	19
Gibt es einen Notfallplan mit definierten Prozessen und Aufgaben im Falle eines Cyberangriffs?	26	19
Haben Sie einen Informationssicherheitsbeauftragten?	25	20
Führt die KI selbstständig folgenreiche Aktionen aus (oder hat stets ein Mensch das letzte Wort)?	17	6
Ist Ihr Unternehmen nach ISO/IEC 27001 zertifiziert?	15	20
Haben Sie eine security.txt auf Ihren Webseiten platziert?	6	18
Setzen Sie in Ihrem Unternehmen eine Blockchain ein?	0	19
Ist Ihr Unternehmen nach BSI Grundschutz zertifiziert?	0	20

Tabelle 1: Prozentsatz der Ja-Stimmen

Frage	Stichproben-umfang	Minimum	Maximum	Durchschnitt	Standard-abweichung
Welche Antivirensoftware setzen Sie ein?	17	4	5	4,88	0,33
Nutzen Sie Cloud-Lösungen von Drittanbietern?	17	3	5	4,82	0,53
Zu welchen Bereichen haben Kunden und Besucher Zugang? Sind sie je unbeaufsichtigt?	18	3	5	4,72	0,57
Setzen Sie in Ihrem Unternehmen künstliche Intelligenz ein?	6	3	5	4,67	0,82
Haben Sie schon von Quantencomputern und deren Gefahren für die Kryptographie gehört?	20	3	5	4,65	0,59
Wurde Ihre Infrastruktur schon einmal einem Penetrationstest unterzogen?	18	3	5	4,61	0,61
In welchen Bereichen setzen Sie KI ein?	5	3	5	4,60	0,89

Hat jeder Mitarbeiter ein eigenes Benutzerkonto (oder teilen sie sich ein gemeinsames Konto)?	20	4	5	4,60	0,50
Welche Firewalls setzen Sie ein?	19	3	5	4,53	0,84
Welche Betriebssysteme setzen Sie ein?	20	3	5	4,50	0,83
Setzen Sie alte Software ein, die keine Sicherheitsupdates mehr erhält?	20	3	5	4,50	0,69
Haben Sie einen Datenschutzbeauftragten?	19	3	5	4,47	0,70
Setzen Sie Zwei-Faktor-Authentisierung ein?	20	2	5	4,45	0,89
Ist Ihr Unternehmen ISO/IEC 27001 zertifiziert?	19	2	5	4,42	0,84
Wurden Sie schon einmal Opfer einer Cyberattacke?	15	3	5	4,40	0,83
Gibt es Richtlinien zur physischen Sicherheit?	20	3	5	4,35	0,81
Wie oft überprüfen Sie ob neue Sicherheitsupdates existieren und spielen diese ein?	16	2	5	4,31	0,95
Machen Sie regelmäßig Backups Ihrer Daten?	20	1	5	4,30	1,13
Haben Sie sich bereits Gedanken gemacht, wie Quantencomputer Ihr Unternehmen beeinflussen wird?	17	2	5	4,24	0,83
Ist Ihr Unternehmen nach BSI Grundschutz zertifiziert?	19	2	5	4,21	0,79
Führt die KI selbstständig folgenreiche Aktionen aus (oder hat stets ein Mensch das letzte Wort)?	5	3	5	4,20	0,84

Gibt es eine Passwort-Richtlinie?	20	1	5	4,15	1,14
Wird die Passwortrichtlinie technisch forciert?	16	1	5	4,13	1,45
Wird die Infrastruktur überwacht?	19	2	5	4,11	1,20
Können die Backups von einem Angreifer überschrieben werden?	19	2	5	4,11	0,94
Setzen Sie IoT-Geräte ein?	13	1	5	4,08	1,32
Haben Sie einen Informationssicherheitsbeauftragten?	19	2	5	4,05	0,97
Dürfen Ihre Mitarbeiter nur auf für sie relevante Daten und Dienste zugreifen (oder hat jeder Zugriff auf alles)?	19	2	5	3,89	1,15
Haben Sie eine security.txt auf Ihren Webseiten platziert?	19	2	5	3,89	0,90
Haben Ihre Mitarbeitenden schon einmal eine IT-Sicherheitsschulung erhalten?	20	1	5	3,75	1,25
Gibt es einen Netzwerkplan, bei dem sauber dokumentiert ist, welche Maschinen existieren, wer mit wem kommuniziert und welche Ports geöffnet sind?	19	1	5	3,68	1,16
Ist das Netzwerk segmentiert (oder hängen alle Geräte in einem großen Netzwerk zusammen)?	19	1	5	3,68	1,34
Nutzen Sie eine Methode zur Bedrohungsanalyse?	20	1	5	3,30	0,98
Gibt es einen Notfallplan mit definierten Prozessen	19	1	5	2,95	1,35

und Aufgaben im Falle eines Cyberangriffs?					
Wurde die KI selbst entwickelt (oder eingekauft)?[3]	-	-	-	-	-
Setzen Sie in Ihrem Unternehmen eine Blockchain ein?	-	-	-	-	-
In welchen Bereichen setzen Sie eine Blockchain ein?	-	-	-	-	-
Warum haben Sie sich in diesem Fall für eine Blockchain entschieden?	-	-	-	-	-

Tabelle 2: Einschätzung des Verbesserungspotenzials

[3] Bei den letzten vier Zeilen der Tabelle (Fragen) liegen zu wenige Antworten vor, um Einschätzungen treffen zu können.