Institut für Technologiequalität

Ein ITQ-Produkt

Ransomware Checkup ITQ

Geprüfte Infrastruktur - Anforderung Mittelstand

Basis RWCv3

Geprüftes Unternehmen

Musterunternehmen GmbH

Inhalt

Audit Facts

Geprüftes Unternehmen	Musterunternehmen GmbH
Ansprechpartner	Bert Stromberg / stromberg@versicherung.de / 0172 8886854
Prüfzeitraum	03.02.2025 - 03.02.2025
Berichtsnummer	B459.894
ITQ-Partner	ITQ GmbH
Auditor	Antonia Gotschke
Auditor-Kennung	A484.162
Verteiler	Capitol Vesicherung, Stromberg
Audit-Typ	Ist Analyse
Prüforte	Capitol GmbH Maurer Straße 28 765494 Finsdorf

Disclaimer

Die im Folgenden dargestellten Anforderungen sowie präventiven und reaktiven Maßnahmen wurden unter Beachtung der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik, der unterschiedlichen Cyber-Versicherer, der Landesdatenschutzbehörden und diverser IT-Experten erstellt. Die ITQ GmbH hat nach bestem Wissen und Gewissen einen Prüfkatalog nebst einem Soll-Ist Vergleich für klein- und mittelständische Unternehmen (KMU) als Zielgruppe erstellt. Wir weisen ausdrücklich darauf hin, dass auf Grund besonderer Umstände und individueller Eigenschaften Ihres Unternehmens eventuell weitere Anforderungen gestellt werden müssten, um ein angemessenes Sicherheitsniveau zu erreichen und daher entsprechend weitere Maßnahmen umzusetzen wären. Grundlage der Ermittlung, inwieweit die Anforderungen erfüllt sind oder nicht, sind neben persönlichen Gesprächen bzw. Befragungen auch weitere Maßnahmen wie Aktivitäts- und Messdatenanalyse, Einsichtnahme, Dokumentationsprüfung und Unterlagensichtung. Die Vollständigkeit und Richtigkeit von Aussagen und Angaben kann von uns nicht geprüft werden, so dass wir keine Haftung für die Vollständigkeit und Richtigkeit des aus diesen Angaben erstellten Berichtes bzw. der Maßnahmenempfehlungen übernehmen können.

Vorwort

Herzlichen Glückwunsch!

Sie sind den ersten wichtigen Schritt gegangen, indem Sie sich mit dem Thema Ransomware konkret befassen und das Ziel verfolgen, die diesbezügliche Sicherheit in Ihrem Unternehmen erheblich zu verbessern und Ihre wichtigsten Unternehmenswerte sowie Geschäftsprozesse zu schützen. Sie haben bestätigt, dass ein Prozess zur Verbesserung des Schutzniveaus initiiert wurde und können dies nachweisen.

Im weiteren Verlauf des Prüfberichtes werden wir Ihnen die nächsten Schritte aufzeigen und welche Empfehlungen wir bezüglich der Vorgehensweise aussprechen. Auf Wunsch stehen wir Ihnen während des gesamten Verfahrens prozessbegleitend zur Seite.

Wir freuen uns auf eine gute Zusammenarbeit!

Einleitung

Die Bedrohungslage durch Ransomware bzw. Verschlüsselungstrojaner, die ganze Datenbestände eines Unternehmens unbrauchbar machen können, steigt jedes Jahr weiter an. Nicht nur Großkonzerne sind Opfer von Cyberangriffen, sondern auch vermehrt öffentliche Einrichtungen sowie kleine und mittelständische Unternehmen, die in der Regel nur schwache Vorbereitungs- und Schutzmaßnahmen umgesetzt haben, um sich gegen diese Bedrohung abzusichern. Viele kleinere Unternehmen sind immer noch der Auffassung, bei ihnen sei nichts zu holen. Tatsächlich geht es den Tätern für gewöhnlich nur um schnelles Geld und geringen Arbeitsaufwand, den man mangels geeigneter Schutzmaßnahmen in der Tat als gering einschätzen muss. Aufgrund der verheerenden Folgen einer Komplettverschlüsselung des gesamten Datenbestandes ist es zwingend erforderlich, vorhandene Sicherheitslücken oder fehlende Schutzmaßnahmen ausfindig zu machen und zu schließen. Zu beachten ist bei einem derartigen Angriff auch immer, dass der Täter nicht nur Daten verschlüsselt, sondern häufig auch mit einer Veröffentlichung vertraulicher Informationen bei Nichtzahlung droht.

Mit dem ITQ Ransomware Checkup wird ebendieser Bedrohungslage Rechnung getragen und ganz spezifische Anforderungen geprüft sowie Maßnahmenempfehlungen ausgesprochen, um den Schutz gegen diese Form von Schadprogrammen wesentlich zu erhöhen.

Prüfungsumgebung

Prüfobjekt ist das Unternehmen Capitol GmbH an seinem Standort in Finsdorf. Zum Informationsverbund gehören alle Prozesse, Verfahren und Systeme, die für die Abwicklung der Geschäftsprozesse erforderlich sind. Derzeit sind 100 Arbeitsplätze, 15 Server, ca. 20 mobile Endgeräte (Smartphones und Tablets) sowie weitere Netzwerkkomponenten (Switches, Firewalls) im Einsatz. Derzeit werden keine cloudbasierten Dienste genutzt. Geprüft werden die beschriebenen Objekte auf Grundlage der Empfehlungen u.a. des BSI.

Management Summary

Übersicht der durchgeführten Arbeiten

Im Rahmen des ITQ-Ransomware Checkups wurde durch unterschiedliche Auditmethoden der aktuelle Stand des Sicherheitsniveaus vor Ransomware-Angriffen ermittelt. Maßstab für die Bestimmung dieses Sicherheitsniveaus ist ein Anforderungskatalog, der von der ITQ für kleine und mittlere Unternehmen entwickelt wurde und insgesamt 84 Fragen umfasst, die 5 unterschiedlichen Prüfgruppen zugeordnet wurden.

Die jeweiligen Ergebnisse der Prüffragen können dem Diagramm „Erfüllungsgrad" entnommen werden. Es wurde für alle festgestellten Mängel oder Sicherheitslücken eine Liste mit Maßnahmenempfehlungen erstellt, nach deren Erledigung eine Risikobeseitigung oder zumindest eine angemessene Risikoreduzierung sichergestellt ist. Der Empfehlungskatalog priorisiert zwar einzelne Maßnahmen mit einem erhöhten Risikowert, gleichwohl sollte die Reihenfolge nicht als verbindlich betrachtet, sondern immer einer individuellen Bewertung unterzogen werden. Eine detaillierte Übersicht der Prüfungsergebnisse zu den einzelnen Fragen kann dem beigefügten Bericht entnommen werden. Dort wird aufgezeigt, wie der aktuelle Status beim geprüften Unternehmen ist und welche Maßnahmen umzusetzen wären, sollte ein Mangel festgestellt worden sein.

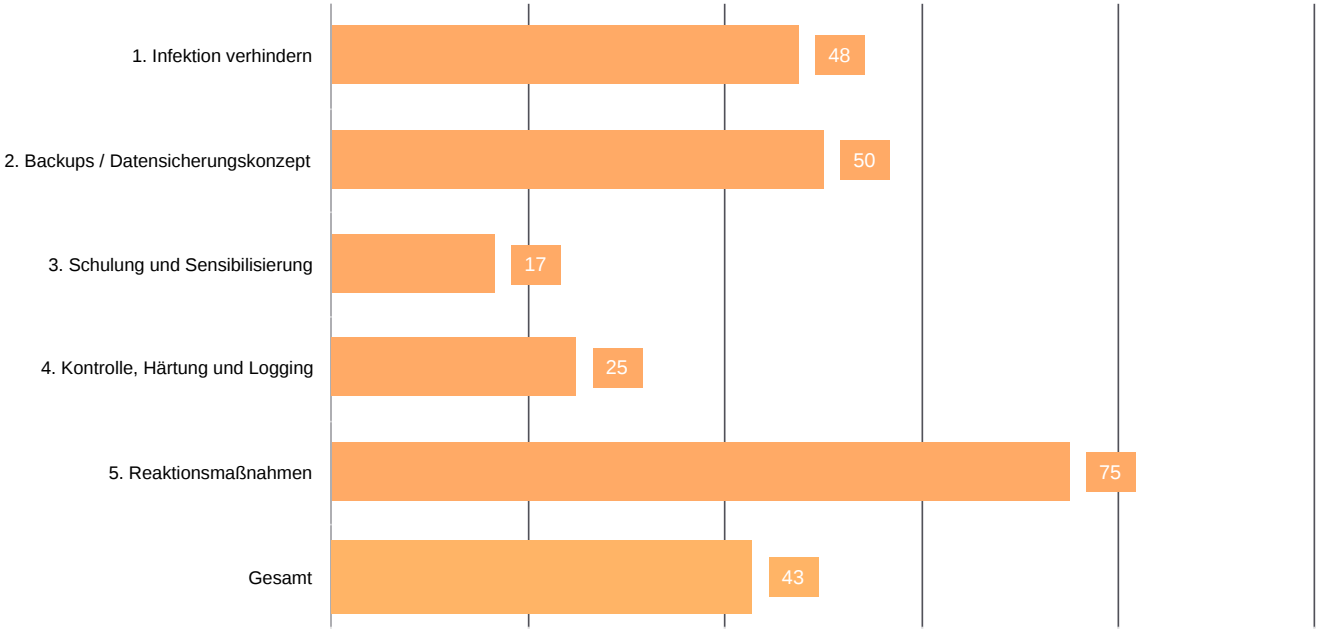
Die ITQ hat zudem nach eigenem Ermessen eine erste Risikoabschätzung vorgenommen und das Ergebnis als Orientierungshilfe zu Verfügung gestellt. Abschließend wird in einem Fazit eine Gesamtbewertung der unternehmerischen IT-Infrastruktur vorgenommen und der Schutz gegen Ransomware-Angriffe bewertet.

Die Ergebnisse der Prüfung wurden durch folgende fettmarkierten Auditmethoden festgestellt:

Dokumentationsprüfung	Aktivitätsanalyse	Messdatenanalyse
Ansichtsnahme	**Befragung**	Unterlagensichtung

Erfüllungsgrad

Nachfolgend erhalten Sie eine grafische Übersicht der geprüften Themenbereiche unterteilt in Prüfgruppen. Der Erfüllungsgrad wird in Prozent angegeben, wobei 100 % einer vollständigen Umsetzung der gestellten Anforderungen entsprechen.



Risikobewertung

Bitte beachten Sie:
Bei der Risikobewertung handelt es sich um eine vom ITQ-Gremium erstellte Ermessensentscheidung. Grundlage der Bewertung ist die „Risiko-Matrix“, die Sie unter „Anhänge“ in diesem Dokument finden können. Selbstverständlich können Sie Risiken nach eigenem unternehmerischen Ermessen neu bewerten und zu einer anderen Entscheidung kommen, indem die individuellen Umstände des Betriebes berücksichtigt werden.

2740

Wurde im Rahmen des ITQ-Ransomware Checkups mindestens ein Problem mit sehr hohem Risikograd festgestellt, fällt die Risikobewertung in ihrer Gesamtheit „sehr hoch“ aus. Probleme mit hohem Risikograd sollten unternehmensseitig bei der Umsetzung besonders berücksichtigt und die korrespondierenden Maßnahmen vorrangig umgesetzt werden.

Fazit

Das Unternehmen erreicht insgesamt ein Ergebnis von X Prozent der empfohlenen Anforderungen. Der Zustand muss/kann als mangelhaft/unterdurchschnittlich/durchschnittlich/gut/sehr gut bewertet werden.

Im Bereich der Infektionsverhinderung fehlt es allem voran an einem organisierten Patchmanagement, wodurch es entweder zur verspäteten Installation von Sicherheitsupdates kommt oder ganz ausbleibt.

Bei der Minimierung der Angriffsfläche wurden bislang wichtige Einstellung nicht vorgenommen, sodass zusätzliche Gefahren geschaffen werden, die bei der Nutzung der Browser oder nicht freigegebener Software entstehen.

Zur Steigerung der E-Mailsicherheit müssen noch weitere Schutzmaßnahmen umgesetzt werden, die bislang nicht implementiert sind. Insbesondere Makros und Skripte in Dokumenten sollten hierbei berücksichtigt werden. Zudem sollte geprüft werden, ob und inwieweit das Filtern von Anhängen erweiterungsbedürftig ist.

Die Zugriffsrechte auf Datenspeicherorte sollten so restriktiv wie möglich ausgestaltet werden, um bei einer Kompromittierung eines Kontos die negativen Folgen so gering wie möglich zu halten. Insbesondere administrative Accounts müssen durch die Verwendung komplexer Passwörter und einer Multi-Faktor-Authentifizierung besonders geschützt werden.

Achten Sie darauf, dass entsprechende Schutzmaßnahmen für Zugriffe auf exponierte Systeme umgesetzt wurden und regelmäßige Kontrollen stattfinden, da von diesen ein erhöhtes Risiko ausgeht.

Im Bereich des Virenschutzmanagements sind Mängel vorhanden, die es zu beseitigen gilt. Allen voran muss auf die Aktualität der Virenschutzsignaturen geachtet werden und ein vollumfänglicher Schutz aller Systeme gewährleistet sein.

Die Konfiguration der Firewall muss genauer überwacht werden, das bezieht sich sowohl auf Sicherheitsupdates als auch auf die allgemeine Grundkonfiguration und Ports. Zudem empfehlen wir die Überwachung der Firewall-Protokolle mittels einer SIEM-Lösung.

Die erforderlichen Anforderungen an ein ganzheitliches Datensicherungskonzept wurden bislang nicht erfüllt. Es sind dringend Sicherungsintervalle, Verantwortlichkeiten und alle einhergehenden Routineaufgaben verbindlich zu definieren sowie zu dokumentieren.

Es ist elementar, dass eine zusätzliche Datensicherung existiert, die weder in der Cloud liegt noch aus dem internen Netz erreichbar ist, um einen Schutz gegen Brand und eine Kompromittierung des Netzwerkes zu erreichen.

Hauptursache für den Befall mit Ransomware ist das Verhalten von Mitarbeitern, die entweder unachtsam auf eine E-Mail klicken oder fragwürdige Webseiten besuchen. Daher sollte dringend ein Schulungskonzept entworfen werden und mindestens jährlich, besser noch öfter, Schulungs- und Sensibilisierungsmaßnahmen durchgeführt werden. Insbesondere bei neuen Mitarbeitern ist darauf zu achten, dass diese schnellstmöglich auf den aktuellen Stand der Wissensvermittlung gebracht werden.

Relevante Systeme sollten kontinuierlich durch geeignetes Monitoring überwacht werden. Eine dauerhafte Inventarisierung aller IT-Assets ist grundlegende Voraussetzung. Vor dem produktiven Einsatz sind Systeme entsprechend zu härten. Netzwerke sollten angemessen segmentiert werden, um eine Ausbreitung von Schadsoftware zu verhindern. Das Aufzeichnen von Ereignissen in Log-Systemen erleichtert späteres Erkennen von Angriffen.

Kommt es zum Ernstfall, sollte dringend ein passendes Notfallkonzept vorhanden sein und Pläne vorliegen, was die genauen Schritte sind, um kurzfristig den Normalzustand wiederherstellen zu können. Daneben sollten Überbrückungsmaßnahmen für den Zeitraum skizziert werden, bis der operative Betrieb wieder den Normalzustand erreicht hat.

Maßnahmenempfehlungen

Die Maßnahmenempfehlungen sind – unabhängig ihrer Zugehörigkeit zu Prüfpunkten und Prüfgruppen – gemäß des Risikograd des jeweiligen Problems aufgelistet, wobei innerhalb des Risikograd keine weitere Sortierung stattfindet. Die Liste ist als erster Umsetzungsplan zu betrachten, kann jedoch auch individuell an das Unternehmen angepasst werden.

Probleme mit **hohem Risikograd** sind rot gekennzeichnet.
Probleme mit **mittlerem Risikograd** sind orange gekennzeichnet.
Probleme mit **niedrigem Risikograd** sind grau gekennzeichnet.

Prüfpunkt	Bezeichnung
1.1	Absicherung der Remote-Zugänge
1.2	Sicherheit der Admin-Konten verbessern
1.4	Sicherheit von E-Mails und Spam-Schutz
1.5	Schutz von E-Mails und Dokumenten
1.6	Client-Sicherheit
1.7	Patchmanagement verbessern
1.8	Virenschutzlösung konfigurieren
1.9	Virenschutzlösung konfigurieren
2.1	Datensicherungskonzept verbessern
2.2	Backup-Prozess überarbeiten
3.1	Schulung der Mitarbeiter erweitern
4.1	Kontrollmaßnahmen

Prüfpunkt	Bezeichnung
4.2	Härtungsmaßnahmen
4.3	Logging
5.1	Notfallmanagement umsetzen

Prüfpunkt	Bezeichnung

Nächste Schritte

Es wird empfohlen, die erstellten Maßnahmen Schritt-für-Schritt im Rahmen eines kontinuierlichen Prozesses umzusetzen, da sich die Verwirklichung in einem großen Schritt in der Praxis als zu ehrgeizig erwiesen hat. Die Maßnahmenempfehlung ist als erster unverbindlicher Umsetzungsplan zu verstehen und soll einen Überblick verschaffen, welche Aufgaben es zu erfüllen gilt. Zunächst sollte eine Einteilung in technische und organisatorische Maßnahmen erfolgen, um eine Zuweisung zu den jeweiligen Fachbereichen zu erleichtern. Im nächsten Schritt ist der jeweilige personelle, finanzielle und organisatorische Ressourcenaufwand zu bestimmen und die Reihenfolge der Umsetzung festzulegen, wobei wir folgende Empfehlungen und Hinweise geben möchten, welche Maßnahmen vorrangig umzusetzen sind:

- ✓ Maßnahmen mit Flächenwirkung, d.h. es werden gleichzeitig mehrere Anforderungen erfüllt
- ✓ Maßnahmen, die ein hohes Risiko abstellen
- ✓ Maßnahmen im organisatorischen Bereich sind kurzfristig und günstig zu erledigen
- ✓ Maßnahmen für Bereiche mit auffallend vielen Mängeln
- ✓ Maßnahmen, die zur Erfüllung einer anderen erforderlich sind

Bei der Budgetierung sollte beachtet werden, dass Informationssicherheit als Prozess zu verstehen ist und Maßnahmen mitunter kontinuierlich wiederholt werden müssen. Ordnen Sie die unterschiedlichen Maßnahmen thematisch und definieren Sie Verantwortlichkeiten für deren Umsetzung.

Die nachfolgenden Korrekturmaßnahmen sind nicht nur ein probates Mittel, um Ransomware-Befall zu verhindern, sondern auch weitere Angriffe oder andersartige Schadprogramme abzuwehren.

Prüfgruppen und Prüfpunkte

Es folgt eine Aufführung der geprüften Bereiche sowie der konkreten Maßnahmen zur Beseitigung von Nichtkonformitäten. Die Reihenfolge der Abschnitte stellt keine Priorisierung dar, sondern orientiert sich an den jeweiligen geprüften Themenbereichen. Daher sollte jedes Unternehmen die zutreffenden Maßnahmen identifizieren und eigenständig hinsichtlich der Umsetzungsreihenfolge priorisieren.

1. Infektion verhindern

1.1 Remote-Zugänge sichern

Status Das Management der exponierten Systeme und Remote-Zugänge entspricht nur teilweise den gestellten Anforderungen. Insbesondere Zugänge, die von extern genutzt werden können oder Systeme, auf die von außerhalb zugegriffen werden kann, sind ein hoher Risikofaktor. Es muss daher sichergestellt sein, dass zusätzliche Maßnahmen zur Absicherung umgesetzt und regelmäßige Kontrollen durchgeführt werden.

Kennung **Korrekturmaßnahmen**

1.1.1 Exponierte Systeme sollten für ein Login nicht auf einem Faktor allein basieren, sondern einen zweiten Faktor zur Authentisierung verwenden. Dies gilt insbesondere für VPN-Zugänge, Access Portale usw.

1.1.2 Es sollten regelmäßig Penetrationstest von externer Stelle durchgeführt werden.

1.2 Sicherer Umgang mit Administrator Accounts

Status Die geforderten Präventionsmaßnahmen zum Schutz privilegierter Konten wurden nur teilweise implementiert. Administrative Konten sind aufgrund ihrer weitreichenden Rechte und Zugriffsmöglichkeiten ein besonders beliebtes Angriffsziel, da sich mit deren Kompromittierung häufig das gesamte Netzwerk übernehmen lässt.

Kennung **Korrekturmaßnahmen**

1.2.1 Es muss eine schriftliche Arbeitsanweisung geben, in der eine Nutzung privilegierter Accounts zu allgemeinen Zwecken wie Surfen oder Abrufen von E-Mails untersagt ist.

1.2.2 Setzen Sie dedizierte Kennwörter für jedes System ein und deaktivieren Sie den Built-In Administrator.

1.2.3 Setzen Sie, wo immer es möglich ist, für den Zugang zu extern nutzbaren Systemen und Web-Diensten, wie z.B. Clouddiensten eine Zweifaktor Authentisierung ein.

1.2.4 Verwenden Sie zur Administration Mitglieder übergeordneter, spezieller Gruppen ohne administrative Berechtigung auf die Domäne. Setzen Sie, soweit möglich und angemessen, für die Administration von Domänen bzw. der Active Directory gesondert gesicherte Arbeitsstationen / Privileged Access Workstations (PAW) ein.

1.2.5 Es sollten für Tätigkeiten in Cloud-Umgebungen eigene Cloud-Administratorkonten genutzt werden, um den Schaden beim Befall mit Ransomware zu minimieren.

1.3 Datenspeicherorte

Status Die Anforderungen für die Absicherung der Datenspeicherorte wurden umgesetzt, so dass die Ablage der unternehmenskritischen Daten sichergestellt ist und eine restriktive Zugriffspolitik umgesetzt wurde.

1.4 Behandlung von E-Mails / Spam auf dem Server

Status Die Schutzmaßnahmen zur Reduzierung der Gefahren von Schadprogrammen in E-Mails und des Eingangs von Spam-Nachrichten wurden nicht vollständig umgesetzt. Häufigste Ursache für eine Infektion mit einem Virus, ist das Öffnen einer E-Mail mit gefährlichen Inhalten. Es muss daher bereits der Eingang einer verdächtigen Nachricht in das Postfach des Benutzers unterbunden werden, um so Gefahren durch fahrlässiges oder unachtsames Verhalten zu unterbinden. Für weiterführende Informationen beachten Sie den Hinweis unter Präventionsmaßnahmen 5.1.4 im BSI Dokument.

Kennung **Korrekturmaßnahmen**

1.4.1 Implementieren Sie SPF (Sender-Policy-Framework).

1.4.2 Es wird empfohlen, DKIM und DMARC zur weiteren Verhinderung unerwünschter E-Mails zu aktivieren. DMARC sollte nach einer Erprobungsphase mit einer „None"-Policy zur späteren Auswertung und Vermeidung von Seiteneffekten umgesetzt werden.

1.4.3 Lehnen Sie die Annahme von E-Mails mit internem Absender (SMTP-Envelope und From-Header) von externer Stelle ab. (Anti-Spoofing)

1.4.4 Anwender sollten URLs aus E-Mails als HTML-Links nicht direkt erhalten. Diese sollten durch weitere Absicherungen wie Safelinks geschützt werden, oder der Anwender muss diese bewusst manuell in seinen Browser überführen.

1.5 Behandlung von E-Mails und Dokumenten auf dem Client

Status Die Anforderungen, um Gefahren von Schadprogrammen in Makros oder aktiven Inhalten vorzubeugen, wurden nur teilweise umgesetzt. Hauptträger von Schadprogrammen sind E-Mails oder Office-Dokumente mit ausführbaren Inhalten, die entweder automatisiert oder durch einen unbedarften Benutzer aktiviert werden. Durch entsprechende Maßnahmen muss verhindert werden, dass diese zum Benutzer gelangen oder eine Ausführung möglich ist.

Kennung **Korrekturmaßnahmen**

1.5.1 Nehmen Sie Einstellungen von, dass E-Mails, die nicht aus Ihrem Unternehmen kommen, als „Extern“ getagged werden.

1.5.2 Stellen Sie sicher, dass das Nachladen von Dateien, wie Bilder und Skripte nicht automatisch geschieht und erst nach manuellem Aktivieren durch den Benutzer erfolgt.

1.5.3 Definieren Sie vertrauenswürdige Orte und Herausgeber für Makros.

1.5.4 Für alle im Unternehmen genutzten Makros muss eine digitale Signatur erstellt werden.

1.6 Client-Sicherheit

Status Es wurden nicht alle erforderlichen Maßnahmen zur Reduzierung der Angriffsfläche für Cyberattacken umgesetzt. Insbesondere das Internet ist direkt nach der E-Mail die zweitgrößte Infektionsquelle für Schadprogramme. Überflüssige Plugins und automatisiertes Ausführen von Skripten und Anwendungen, können mitunter dazu führen, dass bereits beim Besuchen einer Webseite im Hintergrund unbemerkt Schadcode installiert wird.

Kennung **Korrekturmaßnahmen**

1.6.1 Entfernen Sie alle nicht benötigten Browser-Plugins, wie beispielsweise Flash, Java und Silverlight.

1.6.2 Erstellen Sie eine Checkliste mit Vorgaben zur Grundkonfiguration der Clients und notwendiger Schutzmaßnahmen sowie dem Life-Cycle-Management.

1.6.3 Die Verwendung von privaten Endgeräten muss in einer Arbeitsanweisung geregelt und untersagt werden.

1.6.4 Zur Verwaltung der Smartphones muss eine MDM-Lösung eingesetzt werden.

1.7 Softwareupdates

Status Die gestellten Anforderungen wurden nur teilweise umgesetzt, insofern muss das Patchmanagement innerhalb des Unternehmens als lückenhaft bewertet werden. Werden bestehende Sicherheitslücken in Systemen und Anwendungen nicht geschlossen, können diese durch Cyberkriminelle als Einfallstor in das interne Netzwerk genutzt werden. Häufig werden diese Lücken im Internet veröffentlicht und Angreifer können danach gezielt suchen, welche Unternehmen diese Schwachstellen noch nicht geschlossen haben.

Kennung **Korrekturmaßnahmen**

1.7.1 Spielen Sie immer unverzüglich alle Sicherheitsupdates für Systeme ein, die aus dem Internet erreichbar sind, wenn der Hersteller neue Patches bereitstellt.

1.7.2 Alle Anwendungen, mit denen Inhalte aus dem Netzwerk bzw. dem Internet geöffnet werden können, müssen immer unverzüglich aktualisiert werden, wenn der Hersteller neue Sicherheitsupdates bereitstellt.

1.8 Virenschutz

Status Das Unternehmen hat den geforderten Schutz gegen Schadprogramme nur teilweise implementiert und erfüllt die gestellten Anforderungen nicht vollständig. Ein funktionierendes Virenschutzmanagement ist unumgänglich, um gegen Ransomware gewappnet zu sein. Lücken können besonders schwerwiegende Folgen haben und dazu führen, dass Viren nicht erkannt werden, wenn die Aktualität der Software nicht sichergestellt ist.

Kennung **Korrekturmaßnahmen**

1.8.1 Alle Systeme müssen ausnahmslos mit einem Virenschutz-Programm aus dem Enterprise Bereich ausgestattet sein.

1.8.2 Stellen Sie sicher, dass alle eingesetzten AV-Programme und Virensignaturen auf dem aktuellen Software-Stand sind.

1.9 Firewall

Status Es gibt Abweichungen vom Stand der Technik und regelmäßig auszuführenden Aufgaben, diese beziehen sich auf regelmäßig zu prüfende Punkte.

Kennung **Korrekturmaßnahmen**

1.9.1 Prüfen Sie regelmäßig, ob die Firewall-Regeln noch Ihrem Schutzbedarf entsprechen und ob Ihre Firewall regelmäßige Sicherheitsupdates bekommt.

1.9.2 Stellen Sie sicher, dass eine regelmäßige Prüfung der Firewall-Protokolle stattfindet.

2. Backups / Datensicherungskonzept

2.1 Datensicherungskonzept

Status Das vorliegende Datensicherungskonzept entspricht nur teilweise den gestellten Anforderungen und ist veraltet bzw. wichtige Inhalte fehlen. Ein ordnungsgemäßes Datensicherungskonzept ist nicht nur Grundlage, um einen regelmäßigen Soll-Ist-Vergleich anstellen zu können, sondern gleichzeitig auch die Arbeitsanweisung für den Administrator, wie der Backup-Prozess zu gestalten ist.

Kennung **Korrekturmaßnahmen**

2.1.1 Legen Sie im Datensicherungskonzept für jedes System fest, welche Daten gesichert werden müssen und welches Backup-Verfahren anzuwenden ist.

2.1.2 Definieren Sie als Unternehmensleitung die Sicherungszeitpunkte der Systeme unter der Beachtung ihrer Verfügbarkeitsansprüche bzw. des maximal tolerierbaren Datenverlustes.

2.1.3 Legen Sie klare Verantwortlichkeiten und Stellvertreter für die Aufgaben im Datensicherungsmanagement fest, wie Durchführung des Backups, Erfolgskontrolle und Recovery-Tests.

2.2 Backups

Status Die Ausgestaltung des Backups entspricht nur teilweise den gestellten Anforderungen in Bezug auf Speicherorte, Härtung bzw. Recovery-Tests. Neben der regelmäßigen Datensicherung ist es elementar, dass der Zugriff auf das Backup durch eine Remote-Verbindung nicht möglich sein darf. Angreifer versuchen in der Regel nicht nur die Produktivdaten zu verschlüsseln, sondern auch die Datensicherungen des Unternehmens.

Kennung **Korrekturmaßnahmen**

2.2.1 Führen Sie regelmäßig Rücksicherungstests durch, die nicht nur einzelne Dateien, sondern auch ganze Systeme, wie z.B. virtuelle Maschinen umfassen.

2.2.2 Führen Sie eine Härtung des Betriebssystems des Datensicherungsservers durch.

2.2.3 Stellen Sie sicher, dass der Backup Server außerhalb des Active Directory z.B. in einer eigenen Arbeitsgruppe betrieben wird.

3. Schulung und Sensibilisierung

3.1 Mitarbeitersensibilisierung

Status Die Mitarbeiterschulung wird nicht im erforderlichen Umfang durchgeführt. Statistiken zeigen, dass nahezu jeder zweite Sicherheitsvorfall auf die Fahrlässigkeit oder das unbedarfte Verhalten eines Mitarbeiters zurückzuführen ist. Die beste Firewall oder Virenschutzlösung entfaltet keine Wirkung, wenn die Mitarbeiter falsche E-Mails öffnen, Schadcode aus dem Internet herunterladen oder Passwörter bei Social Engineering-Angriffen an Dritte rausgeben.

Kennung **Korrekturmaßnahmen**

3.1.1 Erstellen Sie eine Benutzerrichtlinie für den sicheren Umgang mit IT-Systemen und lassen sich die Kenntnisnahme durch alle Mitarbeiter bestätigen.

3.1.2 Initiale Schulungen zum Thema Informationssicherheit müssen Bestandteil jedes Onboarding-Prozesses für neue Mitarbeiter sein.

3.1.3 Schulen Sie Ihre Mitarbeiter regelmäßig im sicheren Umgang mit E-Mails, insbesondere woran man Fake-Mails erkennen kann.

3.1.4 Im Schulungsprogramm muss das Thema „sicheres Surfen im Internet und Gefahren von Webseiten“ integriert werden.

3.1.5 Die Mitarbeiter müssen zum Thema „Gefahren durch Social Engineering“ geschult werden.

3.1.6 Benennen Sie einen Ansprechpartner für Mitarbeiter, sollten Zweifel an der Integrität beispielweise einer E-Mail oder Internetseite bestehen, um diese einer fachkundigen Prüfung unterziehen zu lassen.

4. Kontrolle, Härtung und Logging

4.1 Kontrollmaßnahmen

Status Die erforderlichen weiteren Schutzmaßnahmen zur Absicherung gegen Ransomware wurden nur teilweise umgesetzt. Zu einem ganzheitlichen Sicherheitsmanagement gehört es auch, dass Zuständigkeiten klar definiert sind, Logs überwacht und regelmäßige Besprechungen zum Stand der Bedrohungslage durchgeführt werden. Daneben bedarf es der kontinuierlichen Überprüfung der Effektivität von Schutzmaßnahmen.

Kennung **Korrekturmaßnahmen**

4.1.1 Stellen Sie sicher, dass Brute-Force-Attacken durch das Monitoringsystem erkannt und gemeldet werden.

4.1.2 Zumindest im halbjährlichen Turnus muss das Thema Informationssicherheit in einer Besprechung behandelt werden.

4.1.3 Erstellen Sie eine Übersicht aller Informationssicherheitsmaßnahmen und definieren Sie entsprechende Zuständigkeiten.

4.1.4 Erstellen Sie ein Inventar aller Ihrer unternehmensrelevanten Assets und integrieren Sie alle Systeme in das Patchmanagement.

4.2 Härtungsmaßnahmen

Status Die erforderlichen weiteren Schutzmaßnahmen zur Absicherung gegen Ransomware wurden nur teilweise umgesetzt. Zu einem ganzheitlichen Sicherheitsmanagement gehört es auch, dass Zuständigkeiten klar definiert sind, Logs überwacht und regelmäßige Besprechungen zum Stand der Bedrohungslage durchgeführt werden. Daneben bedarf es der kontinuierlichen Überprüfung der Effektivität von Schutzmaßnahmen.

Kennung **Korrekturmaßnahmen**

4.2.1 Prüfen Sie durch regelmäßige Schwachstellen-Scans, ob die Härtungs- und Absicherungsmaßnahmen greifen.

Bemerkung:

4.3 Logging

Status Die erforderlichen weiteren Schutzmaßnahmen zur Absicherung gegen Ransomware wurden nur teilweise umgesetzt. Zu einem ganzheitlichen Sicherheitsmanagement gehört es auch, dass Zuständigkeiten klar definiert sind, Logs überwacht und regelmäßige Besprechungen zum Stand der Bedrohungslage durchgeführt werden. Daneben bedarf es der kontinuierlichen Überprüfung der Effektivität von Schutzmaßnahmen.

Kennung **Korrekturmaßnahmen**

4.3.1 Setzen Sie eine Logging Policy um, die sicherstellt, dass Logs regelmäßig erzeugt und mittels zentralem Log Server sicher gespeichert werden.

4.3.2 Überprüfen Sie regelmäßig die Logs der Log Server auf Auffälligkeiten.

Bemerkung:

5. Reaktionsmaßnahmen

5.1 Reaktionsmaßnahmen

Status Die Reaktionsmaßnahmen auf Sicherheitsvorfälle sind nur unvollständig umgesetzt, so dass mit erheblichen Verzögerungen zu rechnen ist, bis ein Notfall beseitigt worden ist. Die Umsetzung eines funktionierenden Notfallmanagements ist essenziell bei einem Ransomware-Befall, da nur so der mögliche Schaden auf ein Mindestmaß begrenzt werden kann. Ein ungeplantes und unkoordiniertes Vorgehen kann dazu führen, dass sich der Schaden stark erhöht.

Kennung **Korrekturmaßnahmen**

5.1.1 Erstellen Sie einen Alarmierungsrufplan mit allen notwendigen Kontakten, wenn ein Sicherheitsvorfall eintritt. (z. B. Forensiker, IT-Betreuer, Cybersicherheitsbehörde, Cyber-Versicherung)

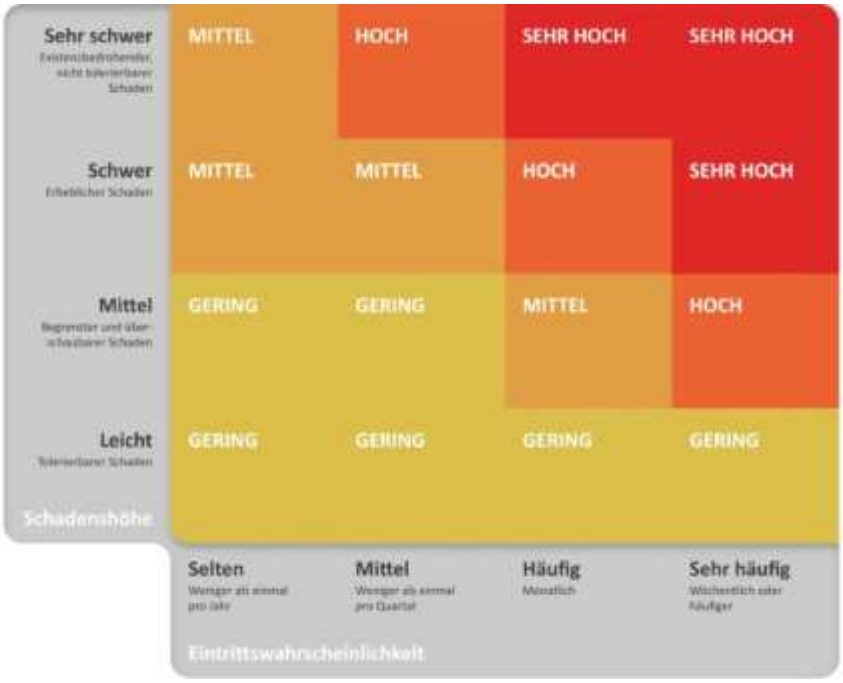
5.1.2 Schaffen Sie eine geeignete Plattform, mit deren Hilfen die unterschiedlichen Personen in einem Notfall kommunizieren können, auch wenn die internen Systeme nicht mehr erreichbar sind. Dort sollte ebenfalls ein Austausch von Dokumenten möglich sein.

Anhänge

Risikomatrix

Risiko-Matrix

Auf Basis der nachfolgenden Risikomatrix wurden die jeweiligen Risikowerte bestimmt, wenn eine spezifische Maßnahme nicht umgesetzt wurde. Der Wert errechnet sich aus einer Multiplikation zwischen Eintrittswahrscheinlichkeit eines Schadens mit der erwarteten Schadenshöhe. Der Umgang mit aufgedeckten Risiken sollte einer weiteren Betrachtung unterzogen werden, wobei unterschiedliche Behandlungsmethoden von der Risikovermeidung, über die -minderung oder -transfer bis hin zur -akzeptanz gängig sind.



.rendered-md-container h6{ color: #111; } .rendered-md-container .badge-contain{ width: 500px; position:relative; } .rendered-md-container .badge-contain [dlelement=BadgeText1]{ position: absolute; top: 90px; left: 10px; } .rendered-md-container .badge-contain [dlelement=BadgeText2] { position: absolute; top: 125px; left: 10px; } .rendered-md-container .badge-contain [dlelement=BadgeText1] input{ background: #ffffff33; border-radius: 4px; font-family: Calibri; color: white; border: 0; font-size: 25px; } .rendered-md-container .badge-contain [dlelement=BadgeText2] input{ background: #ffffff33; border-radius: 4px; font-family: Calibri; color: white; border: 0; font-size: 25px; }