STANDORTBESTIMMUNG

Cyber-Risiko Standortbestimmung

Basierend auf dem IKT-Minimalstandard des Bundes.
Entscheidungsgrundlage für Geschäftsleitung und Verwaltungsrat.

Anonymisiertes Beispiel · Treuhand-KMU mit rund 20 Mitarbeitenden

Müller AG

24. April 2026 · Erstellt durch SafeRoute

47 %

HANDLUNGSBEDARF

INHALTSVERZEICHNIS

Inhalt.

01 **Management Summary** 3
Methodik, Gesamtbewertung, Radar-Übersicht und Einschätzung SafeRoute

02 **Risikoanalyse** 5
Kritische, hohe und mittlere Risiken mit Szenarien und Empfohlene Massnahmen

03 **Massnahmenplan** 10
14 priorisierte Massnahmen mit Verantwortlichkeiten und Zeithorizont

04 **Wie weiter** 11
Nächste Schritte und Kontaktinformationen

ANHANG

A **Bereichsanalysen** 12
Detailbewertung aller fünf IKT-Bereiche mit Stärken und Handlungsbedarf

B **Technischer Aussenblick** 18
Analyse Ihrer öffentlich erreichbaren IT-Infrastruktur

C **Methodik** 22
Grundlagen, Reifegradskala und Bewertungslogik

AUF EINEN BLICK

47%
GESAMTBEWERTUNG

16
IDENTIFIZIERTE RISIKEN

14
MASSNAHMEN

65%
ZIELWERT

Ihre Cyber-Sicherheit auf einen Blick.

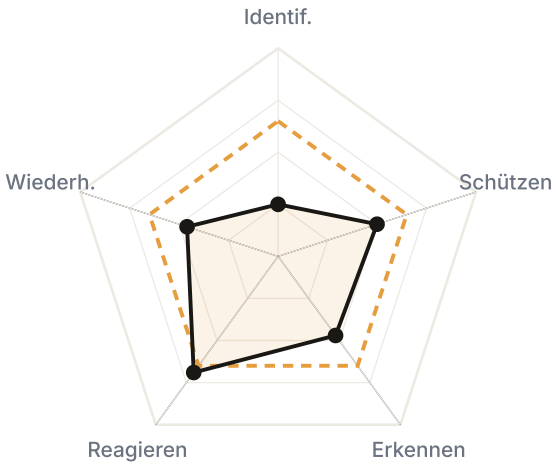
Müller AG hat SafeRoute mit einer unabhängigen Cyber-Risiko Standortbestimmung beauftragt. Diese basiert auf drei Säulen:

Technischer Aussenblick
Analyse der öffentlich erreichbaren IT-Infrastruktur.

Organisatorischer Innenblick
Interview zu Prozessen, Zuständigkeiten und Massnahmen.

Einordnung gegen Standards
Bewertung anhand des IKT-Minimalstandards (108 Massnahmen).

In der Folge finden Sie die Resultate daraus.



● Ist-Zustand - - Zielwert (65%)

47%

GESAMTBEWERTUNG · ZIEL 65%

Identifizieren	Vermögenswerte, Geschäftsumfeld, Governance	25%
Schützen	Zugriffskontrolle, Sensibilisierung, Datensicherheit	50%
Erkennen	Anomalien, Überwachung, Erkennungsprozesse	47%
Reagieren	Reaktionsplanung, Kommunikation, Analyse	69%
Wiederherstellen	Wiederherstellungsplanung, Verbesserungen	46%

Einschätzung SafeRoute.

Im Rahmen dieser Standortbestimmung wurden 108 Massnahmen aus dem IKT-Minimalstandard geprüft. Müller AG erreicht einen Gesamtscore von 47%. Für eine Organisation dieser Grösse und Branche empfehlen wir einen Zielwert von 65%.

Der IT-Betrieb läuft professionell, die Datensicherung ist solide aufgestellt, und für den Ernstfall besteht eine Cyberversicherung. Das ist eine gute Ausgangslage.

Die Bestandsaufnahme zeigt gleichzeitig, dass die organisatorische Seite der IT-Sicherheit bisher wenig adressiert ist, und genau dort liegen die grössten Cyberrisiken. Wie real diese sind, hat Müller AG bereits erfahren: Ein Cyberkrimineller kannte die Firmenübernahme (Meier GmbH), täuschte gezielt Mitarbeitende und brachte sie dazu, Apple-Geschenkkarten zu kaufen. Der Schaden wurde nur durch Zufall verhindert. Solche recherchierten Angriffe werden häufiger und professioneller.

Auch bei der Vorbereitung auf den Ernstfall besteht Nachholbedarf. Der bestehende Notfallplan deckt die technische Seite ab, doch die geschäftliche Priorisierung fehlt: Wenn mehrere Systeme gleichzeitig ausfallen, sollte die Geschäftsleitung entscheiden, welcher Prozess zuerst wiederhergestellt wird – nicht der Techniker. Die technische Analyse hat zudem konkrete Schwachstellen aufgedeckt (offen erreichbare Datenbank, veraltete Software), und der Serverraum ist nach dem Einbruch vor sechs Monaten nach wie vor ohne Zutrittskontrolle.

Aus Governance-Sicht ist das Thema pflichtrelevant. OR Art. 717 verlangt, dass der Verwaltungsrat Risiken kennt und angemessen steuert – Cyberrisiken eingeschlossen. Dasselbe gilt gegenüber der Cyberversicherung: Im Schadenfall prüft sie, ob angemessene Schutzmassnahmen bestanden haben, und kann die Leistung kürzen, wenn grundlegende Sorgfaltspflichten vernachlässigt wurden.

Eine regelmässige, dokumentierte Überprüfung durch eine unabhängige Stelle schafft doppelten Nutzen: Sie zeigt Handlungsbedarf auf und dient als Nachweis der Sorgfaltspflicht. Matthias Berger und SwissIT Partner AG leisten weiterhin gute technische Arbeit – die offenen Punkte liegen in Bereichen, die typischerweise nicht vom IT-Betriebspartner abgedeckt werden. Ähnlich wie es neben dem Treuhänder einen Revisor braucht, braucht es neben dem IT-Betriebspartner eine unabhängige Stelle für die IT-Sicherheit.

Die Standortbestimmung identifiziert 14 konkrete Massnahmen. Einige Quick-Wins lassen sich sofort angehen, die übrigen innerhalb von drei bis sechs Monaten. Bei konsequenter Umsetzung steigt die Gesamtbewertung im ersten Jahr von heute 47% auf rund 63% und im zweiten Jahr voraussichtlich auf 72% – der Wert eines gut aufgestellten KMU.

RISIKOANALYSE

Identifizierte Risiken.

Aus den Lücken in Ihrer Bewertung ergeben sich konkrete Risiken. Für jedes beschreiben wir, was passieren kann und welche Empfohlene Massnahme wir empfehlen.

KRITISCH

3 RISIKEN

Fehlende Datenverschlüsselung & Datenabfluss

Es gibt weder Massnahmen gegen unkontrollierten Datenabfluss noch automatische Integritätsprüfungen, und die Verschlüsselung gespeicherter Daten ist nur teilweise umgesetzt. Kundendaten aus Abacus, technische Zeichnungen und Buchhaltungsdaten liegen auf Servern und Laptops, wobei die Daten auf einem verlorenen oder gestohlenen Laptop ohne Verschlüsselung für jeden lesbar sind, der das Gerät einschaltet. Ohne Kontrolle des Datenabflusses kann zudem jemand grössere Datenmengen per E-Mail oder USB-Stick nach aussen bringen, ohne dass es auffällt. Unter dem neuen Datenschutzgesetz (nDSG) können solche Vorfälle meldepflichtig sein.

EMPFOHLENE MASSNAHME M11

Gespeicherte Daten auf Servern und Laptops sollten verschlüsselt werden, unter Windows mit BitLocker und unter macOS mit FileVault, damit die Daten selbst bei Verlust oder Diebstahl eines Geräts geschützt sind. Zusätzlich sollte eine einfache Regel für den Umgang mit sensiblen Daten eingeführt werden, etwa dass Kundendaten nicht per E-Mail-Anhang an externe Empfänger weitergegeben werden dürfen ohne Freigabe. Als ersten Schritt lohnt es sich zu prüfen, wer aktuell auf welche Daten Zugriff hat.

Fehlende technische Schwachstellenanalysen

Es werden keine regelmässigen technischen Schwachstellenanalysen der von aussen erreichbaren Systeme durchgeführt. SwissIT Partner AG überwacht die Systeme zwar mit Crowdstrike, was vor bekannter Schadsoftware schützt, doch das deckt nur eine Seite ab: Crowdstrike erkennt Angriffe, die bereits stattfinden, während eine technische Schwachstellenanalyse vorher prüft, ob es offene Einfallstore gibt, bevor jemand sie ausnutzt. Die Analyse im Rahmen dieser Bestandsaufnahme hat genau solche Einfallstore gefunden, darunter eine aus dem Internet erreichbare Datenbank, veraltete Software mit bekannten Lücken und abgelaufene Zertifikate. Ohne regelmässige Prüfung wären diese Punkte weiterhin unbemerkt geblieben.

EMPFOHLENE MASSNAHME M7

Regelmässige technische Schwachstellenanalysen der von aussen erreichbaren Systeme sollten eingeführt werden, zum Beispiel quartalsweise. Die Ergebnisse sollten direkt mit SwissIT Partner AG besprochen und mit klaren Fristen für die Behebung versehen werden.

MySQL-Datenbank offen im Internet

Die MySQL-Datenbank auf dem Server 192.0.2.91 ist über Port 3306 direkt aus dem Internet erreichbar, was bedeutet, dass der Zugriff von überall möglich ist. Automatisierte Werkzeuge finden solche offenen Ports innerhalb von Minuten und versuchen sich mit Standard-Passwörtern Zugang zu verschaffen. Bei Erfolg sind die gespeicherten Daten direkt einsehbar, veränderbar und löschbar. Eine Datenbank sollte grundsätzlich nie direkt aus dem Internet erreichbar sein.

EMPFOHLENE MASSNAHME M2

Der Zugang zur MySQL-Datenbank aus dem Internet sollte umgehend gesperrt werden, wozu eine Firewall-Regel genügt, die Port 3306 für externen Zugriff schliesst. Zugriffe auf die Datenbank sollten künftig nur noch aus dem internen Netzwerk oder über eine gesicherte VPN-Verbindung möglich sein, und gleichzeitig sollten die Datenbankpasswörter erneuert werden.

HOCH

5 RISIKEN

Phishing & Social Engineering

Müller AG war bereits Ziel eines gezielten Phishing-Angriffs, bei dem ein Cyberkrimineller die Firmenübernahme als Hebel nutzte. Apple-Geschenkkarten wurden tatsächlich gekauft und nur durch Zufall nicht an den Angreifer weitergeleitet. Das war kein Massen-Spam, sondern ein recherchierter Angriff auf das Unternehmen. Phishing-Mails werden laufend überzeugender und sind heute kaum noch von echten E-Mails zu unterscheiden, weshalb Mitarbeitende ohne die nötigen Kenntnisse solche Angriffe kaum zuverlässig erkennen können. Ein Schulungsprogramm gibt es bisher nicht, und weitere Versuche werden mit Sicherheit folgen.

EMPFOHLENE MASSNAHME M8

Die Schulungen sollten durch regelmässige Phishing-Tests ergänzt werden, bei denen Mitarbeitende kontrollierte Test-E-Mails erhalten, die echte Phishing-Versuche nachahmen. Da Mimecast bereits den E-Mail-Schutz abdeckt, lässt sich diese Infrastruktur auch für solche Tests nutzen. Wer auf eine Test-Mail hereinfällt, wird gezielt nachgeschult, wodurch über die Zeit ein wachsendes Bewusstsein im Team entsteht.

IT-Notfallplanung

Der IT-Notfallplan (v0.2) von SwissIT Partner AG deckt die technische Seite zweckmässig ab, darunter Datensicherung, Offsite-Kopie und Wiederherstellungsabläufe. Was fehlt, ist die geschäftliche Priorisierung: Wenn mehrere Systeme gleichzeitig ausfallen, ist nicht definiert, welches zuerst wiederhergestellt wird. Für Müller AG kann das praktische Konsequenzen haben, denn ein Tag ohne Abacus bedeutet keine Auftragsverarbeitung und keine Rechnungsstellung, während ein Tag ohne E-Mail keine Lieferbestätigungen für Baustellenkunden bedeutet. Ohne vordefinierte Reihenfolge entscheidet im Ernstfall der Techniker nach technischen Kriterien statt die Geschäftsführung nach geschäftlichen. Ebenfalls offen ist der organisatorische Rahmen, also wer mit SwissIT Partner AG koordiniert, wer Kunden informiert und wer über weitere Schritte entscheidet.

EMPFOHLENE MASSNAHME M9

Der bestehende IT-Notfallplan (v0.2) sollte um die geschäftliche Perspektive ergänzt werden. Konkret bedeutet das eine Priorisierung der Systeme nach geschäftlicher Wichtigkeit, damit im Ernstfall klar ist, ob zuerst Abacus, E-Mail oder ein anderes System wiederhergestellt wird. Dazu gehört auch ein organisatorischer Rahmen, der festlegt, wer intern koordiniert, wer mit SwissIT Partner AG kommuniziert und wer Kunden und Partner informiert. Der Plan sollte einmal jährlich in einer Tischübung durchgespielt werden, damit die Abläufe im Ernstfall sitzen.

Veraltete Passwörter

Ein Grossteil der Belegschaft arbeitet noch mit veralteten und schwachen Passwörtern, weil die neue Richtlinie bisher nur für neue Mitarbeitende gilt. Viele bestehende Accounts sind deshalb weiterhin mit Passwörtern geschützt, die möglicherweise einfach zu erraten sind. Angreifer nutzen automatisierte Werkzeuge, die bekannte Passwörter aus früheren Datenlecks systematisch durchprobieren, und wenn ein Mitarbeitender dasselbe Passwort auch bei einem anderen Dienst verwendet hat, etwa einem Online-Shop, der gehackt wurde, kann das Müller AG-Passwort ebenfalls kompromittiert sein.

EMPFOHLENE MASSNAHME M12

Die neue Passwortrichtlinie gilt bisher nur für neue Mitarbeitende, und um die Lücke zu schliessen, sollten alle bestehenden Mitarbeitenden ihre Passwörter einmalig ändern und dabei die neue Richtlinie einhalten. Vorab lässt sich über haveibeenpwned.com prüfen, ob verwendete Passwörter bereits in bekannten Datenlecks aufgetaucht sind, denn diese Seite sammelt Passwörter aus gehackten Diensten und taucht ein Passwort dort auf, ist es für Angreifer bereits bekannt und muss sofort geändert werden. Für Mitarbeitende mit Zugang zu zentralen Systemen lohnt sich zusätzlich ein Passwort-Manager wie 1Password, der sichere Passwörter erzeugt und speichert, sodass sich niemand dutzende komplexe Kombinationen merken muss.

Veraltete Serversoftware (Nginx/Plesk)

Die eingesetzte Serversoftware weist bekannte Sicherheitslücken auf. Konkret ist Nginx 1.24.0 auf den Abacus-Subdomains (Port 9443) von CVE-2023-44487 und CVE-2025-23419 betroffen, während Plesk 18.0.68 auf mueller-treuhand.ch (Port 8443) von CVE-2025-66431 betroffen ist. CVEs sind öffentlich dokumentierte Schwachstellen, was bedeutet, dass Angreifer diese Lücken gezielt und mit frei verfügbaren Werkzeugen ausnutzen können.

EMPFOHLENE MASSNAHME M3

Auf allen Mail- und Webservern sollten die veralteten Verschlüsselungsstandards TLS 1.0 und TLS 1.1 deaktiviert und nur noch TLS 1.2 und höher zugelassen werden. Die veralteten CBC-Chiffren und 3DES sollten durch moderne Verfahren wie AES-GCM oder ChaCha20-Poly1305 ersetzt werden, betroffen sind alle Dienste auf 192.0.2.91 und 192.0.2.146.

Veraltete Verschlüsselungsprotokolle (TLS)

Auf mehreren Systemen werden veraltete Verschlüsselungsprotokolle angeboten, darunter TLS 1.0 und TLS 1.1 auf Mail- und Webservern sowie veraltete CBC-Chiffren und 3DES. TLS ist das Protokoll, das Verbindungen im Internet verschlüsselt, zum Beispiel den E-Mail-Verkehr, und die Versionen 1.0 und 1.1 haben bekannte Schwachstellen, die seit Jahren als unsicher gelten. Betroffen sind bei Müller AG die Mail-Ports und Webdienste auf 192.0.2.91 und 192.0.2.146.

EMPFOHLENE MASSNAHME M13

Cyberrisiken sollten als fester Traktandenpunkt in die bestehenden Management- oder VR-Sitzungen aufgenommen werden, mindestens quartalsweise. Dabei genügt ein kurzer, strukturierter Update mit dem aktuellen Stand der IT-Sicherheit, dem Fortschritt bei offenen Massnahmen und neuen Risiken oder Vorfällen seit dem letzten Bericht, damit die Geschäftsleitung informierte Entscheidungen treffen kann, ohne sich in technische Details vertiefen zu müssen. Das Wissen darüber, welche geschäftskritischen Dokumente und Daten wo liegen, sollte ebenfalls auf GL-Ebene vorhanden sein, weil es im Notfall die Grundlage für Priorisierungsentscheidungen bildet.

MITTEL

8 RISIKEN

IT-Sicherheitsrichtlinie & Risikomanagement

IT-Sicherheitsentscheidungen werden bei Müller AG teils ohne dokumentierte Grundlage getroffen, weil keine Risikomanagement-Strategie existiert. Im normalen Tagesgeschäft mag das funktionieren, doch bei einem Sicherheitsvorfall sieht es anders aus: Wenn innerhalb von Minuten Entscheidungen fallen müssen, etwa ob das Netzwerk getrennt, SwissIT Partner AG alarmiert oder Kunden informiert werden sollen, kann ohne vorab geklärte Zuständigkeiten wertvolle Zeit verloren gehen. Hinzu kommt, dass kein systematischer Überblick besteht, welche gesetzlichen Anforderungen wie das neue Datenschutzgesetz (nDSG) für Müller AG gelten und welche Risiken bewusst in Kauf genommen werden.

EMPFOHLENE MASSNAHME M4

Es sollte eine pragmatische IT-Sicherheitsrichtlinie erstellt werden, die festhält, was die wichtigsten IT-Systeme sind, wer wofür zuständig ist (beispielsweise: Geschäftsführung entscheidet, Matthias Berger setzt um, SwissIT Partner AG betreibt) und welche Regeln für Passwörter, Zugänge und den Umgang mit Daten gelten. Ergänzt werden sollte das Ganze um eine Übersicht der gesetzlichen Anforderungen wie das nDSG und branchenspezifische Vorgaben.

Lieferantensteuerung & SLA

Das Lieferantenrisiko wird noch nicht systematisch gesteuert, ein Punkt, den auch Daniel Isler in seiner Einschätzung "20260110 IT-Sicherheit Müller AG" adressiert hat. SwissIT Partner AG ist als wichtigster IT-Partner für den technischen Betrieb verantwortlich, doch es besteht weder ein SLA noch eine formale Vereinbarung zu Reaktionszeiten oder Sicherheitsstandards. Wenn beispielsweise an einem Freitagabend ein kritisches Problem auftritt, gibt es keine vereinbarte Reaktionszeit und keine Verbindlichkeit, was bis wann behoben sein muss. SwissIT Partner AG würde sehr wahrscheinlich trotzdem helfen, aber "sehr wahrscheinlich" ist keine belastbare Grundlage für den Ernstfall. Das Gleiche gilt für andere Anbieter wie Zucchetti.

EMPFOHLENE MASSNAHME M5

Es sollte eine vollständige Liste aller IT-Dienstleister erstellt werden, darunter SwissIT Partner AG, Metanet, Mimecast, Abacus, Eplan und weitere, jeweils mit deren Rolle, Wichtigkeit und aktuellem Vertragsstatus. Mit SwissIT Partner AG als wichtigstem Partner sollte ein einfaches SLA aufgesetzt werden, das Reaktionszeiten bei Störungen, Erreichbarkeit und Verantwortlichkeiten bei einem Sicherheitsvorfall regelt. Die enge Partnerschaft zwischen SwissIT Partner AG und Müller AG bietet dafür eine gute Basis.

Physischer Zugangsschutz Serverraum

Der Serverraum, in dem die beiden Server, die Firewall und ein Teil der lokalen Datensicherung stehen, ist ohne Zutrittskontrolle zugänglich. Angesichts des Einbruchs ins Gebäude vor sechs Monaten ist das besonders relevant, denn wer physisch an einen Server herankommt, kann Daten kopieren, Hardware beschädigen oder ein Gerät anschliessen, das später Fernzugriff ermöglicht. Solche Eingriffe hinterlassen kaum digitale Spuren und sind schwer nachzuweisen. Auch intern ist der fehlende Schutz relevant, weil jeder Mitarbeitende mit Gebäudezugang den Serverraum betreten kann.

EMPFOHLENE MASSNAHME M10

Der Zugang zum Serverraum sollte physisch überprüft werden, z.B. mit einer Überwachungskamera, welche sicherstellt, dass nur autorisierte Personen Zugang haben und dieser dokumentiert ist. Nach dem Einbruch vor sechs Monaten ist das besonders relevant, da die Server, die Firewall und sonstige IT-Hardware in diesem einen Raum stehen.

E-Mail-Absenderschutz (DMARC/DKIM)

Die E-Mail-Domain mueller-treuhand.ch hat keinen Schutz gegen Absenderfälschung, weil weder DMARC noch DKIM eingerichtet sind. Diese Mechanismen funktionieren wie ein digitaler Absenderstempel, der beweist, dass eine E-Mail wirklich von Müller AG kommt. Ohne diesen Stempel kann jeder im Internet E-Mails versenden, die von @mueller-treuhand.ch zu stammen scheinen, zum Beispiel eine gefälschte Rechnung an einen Kunden, ohne dass der Empfänger die Echtheit prüfen kann. Hinzu kommt, dass Google und Microsoft DMARC zunehmend voraussetzen, wodurch auch echte E-Mails von Müller AG im Spam landen oder gar nicht zugestellt werden können.

EMPFOHLENE MASSNAHME M1

DMARC und DKIM sollten für mueller-treuhand.ch eingerichtet werden, damit nur autorisierte Server E-Mails im Namen von Müller AG versenden können. DKIM lässt sich über Mimecast aktivieren, danach wird DMARC zuerst im Beobachtungsmodus gestartet, um den normalen E-Mail-Verkehr zu analysieren, und anschliessend schrittweise verschärft. Der SPF-Eintrag sollte gleichzeitig bereinigt werden.

TeamViewer-Missbrauch

Bei Müller AG wird regelmässig mit TeamViewer für Fernwartung und Fernzugriff gearbeitet, was TeamViewer-Betrug zu einer relevanten Gefahr macht. Bei dieser verbreiteten Masche rufen Angreifer an, geben sich als IT-Support oder als bekannter Dienstleister aus und bitten darum, eine Fernwartungssitzung zu starten. Weil Müller AG-Mitarbeitende an solche Sitzungen gewöhnt sind, kann eine solche Anfrage schnell als normal eingestuft werden. Sobald die Verbindung steht, sieht der Angreifer alles auf dem Bildschirm und kann Programme starten, Daten einsehen oder Schadsoftware installieren.

EMPFOHLENE MASSNAHME M14

Für die TeamViewer-Nutzung sollten klare Regeln definiert werden: Sitzungen nur bei erwarteten Anfragen von SwissIT Partner AG oder bekannten Partnern starten, nie bei unangekündigten Anrufen, und TeamViewer nach jeder Sitzung beenden, damit kein dauerhafter Fernzugang bestehen bleibt. Ein einfaches Protokoll hilft nachzuvollziehen, wann welche Sitzung stattgefunden hat. Das Thema gefälschte Support-Anrufe sollte zusätzlich ins Schulungsprogramm aufgenommen werden.

Abgelaufenes SSL-Zertifikat

Das SSL-Zertifikat für mehrere Subdomains von mueller-treuhand.ch ist seit dem 26. April 2023 abgelaufen, betroffen sind sieben Subdomains (abacus, archiv, autodiscover, autodiscovery, kontakte, sync und voip auf Port 8443). Ein SSL-Zertifikat bestätigt die Identität eines Servers, vergleichbar mit einem Ausweis, und wenn es abgelaufen ist, zeigen Browser und E-Mail-Programme bei jeder Verbindung eine Sicherheitswarnung an. Das Risiko besteht darin, dass sich Nutzer daran gewöhnen, solche Warnungen wegzuklicken, auch wenn sie einmal berechtigt sind, während automatisierte Systeme die Verbindung möglicherweise ganz blockieren.

EMPFOHLENE MASSNAHME M6

Das IT-Wissen von Matthias Berger sollte schrittweise dokumentiert und auf mehrere Schultern verteilt werden. Ein pragmatischer Ansatz wäre, die wichtigsten Systeme, Zugänge und Abläufe in einem internen IT-Handbuch festzuhalten, einen Stellvertreter zu bestimmen, der zumindest die grundlegenden Abläufe kennt und im Notfall handlungsfähig ist, und Zugangsdaten zentral und sicher zu hinterlegen, zum Beispiel in einem Passwort-Manager, auf den im Ernstfall auch andere autorisierte Personen Zugriff haben.

Wissenstransfer & Schlüsselperson

Das gesamte interne IT- und IT-Sicherheitswissen ist bei Matthias Berger gebündelt. Er kennt die Systeme, die Konfigurationen, die Zugänge und die Abläufe. SwissIT Partner AG kann zwar den technischen Betrieb weiterführen, doch das Wissen darüber, wie die internen Prozesse mit der IT zusammenhängen, welche Sonderlösungen existieren und welche Entscheidungen warum getroffen wurden, ist weder dokumentiert noch auf mehrere Schultern verteilt. Bei einem längeren Ausfall, sei es durch Krankheit, Ferien oder einen Stellenwechsel, kann Müller AG in eine Situation geraten, in der niemand intern weiss, wie bestimmte Systeme konfiguriert sind oder wo wichtige Zugangsdaten liegen.

Cyber-Update Geschäftsleitung

Die Geschäftsleitung hat aktuell keinen strukturierten Überblick über die Cyberrisiken des Unternehmens. Es ist nicht durchgängig bekannt, welche geschäftskritischen Dokumente und Daten wo liegen, wie der aktuelle Stand der IT-Sicherheit aussieht oder welche Massnahmen offen sind. Bei einem KMU dieser Grösse ist das nachvollziehbar, weil die Geschäftsleitung nicht jedes technische Detail kennen muss, doch Cyberrisiken sind Unternehmensrisiken: Ein erfolgreicher Angriff kann den Betrieb für Tage oder Wochen lahmlegen, mit direkten finanziellen Folgen und Reputationsschäden bei Kunden. Ohne regelmässige Einordnung auf Ebene Geschäftsleitung oder Verwaltungsrat fehlt die Grundlage, um informierte Entscheidungen über Investitionen, Prioritäten und akzeptable Risiken zu treffen.

MASSNAHMENPLAN

Priorisierte Massnahmen für Ihr Unternehmen.

14	4	6
MASSNAHMEN	QUICK WINS	MONATE HORIZONT

NR.	MASSNAHME	PRIORITÄT	AUFWAND	VERANTWORTLICH	ZEITHORIZONT
M1	DMARC und DKIM einrichten, E-Mail-Schutz vervollständigen QUICK-WIN	Kritisch	Gering	SafeRoute koordiniert direkt mit Mimecast	7 Tage
M2	MySQL-Datenbank absichern QUICK-WIN	Kritisch	Gering	SafeRoute koordiniert direkt mit SwissIT Partner AG	48 Stunden
M3	TLS modernisieren QUICK-WIN	Kritisch	Gering	SafeRoute koordiniert direkt mit SwissIT Partner AG	7 Tage
M4	IT-Sicherheitsrichtlinie erstellen	Kritisch	Mittel	Intern koordiniert direkt mit SafeRoute	90 Tage
M5	Lieferanten-Steuerung mit SLA SwissIT Partner AG aufbauen	Kritisch	Mittel	Geschäftsleitung koordiniert direkt mit SafeRoute	90 Tage
M6	IT-Dokumentation und Stellvertretung aufbauen	Kritisch	Hoch	Intern koordiniert direkt mit SwissIT Partner AG	6 Monate
M7	Regelmässige technische Schwachstellenanalysen einführen QUICK-WIN	Hoch	Gering	SafeRoute koordiniert direkt mit SwissIT Partner AG	Sofort nach Quick-Wins
M8	Awareness-Programm mit Phishing-Simulationen einführen	Hoch	Mittel	SafeRoute koordiniert direkt mit Intern	90 Tage
M9	IT-Notfallplan um Geschäfts-Perspektive erweitern	Hoch	Mittel	SafeRoute koordiniert direkt mit SwissIT Partner AG	90 Tage
M10	Serverraum physisch absichern	Hoch	Mittel	Intern koordiniert direkt mit SafeRoute	90 Tage
M11	Geräteverschlüsselung und Datenabfluss-Regel umsetzen	Hoch	Mittel	SafeRoute koordiniert direkt mit SwissIT Partner AG	90 Tage
M12	Passwörter wechseln und Passwort-Manager einführen	Hoch	Mittel	Intern koordiniert direkt mit SafeRoute	6 Monate
M13	Cyberrisiken als GL-/VR-Traktandum etablieren	Hoch	Mittel	Geschäftsleitung koordiniert direkt mit SafeRoute	90 Tage
M14	TeamViewer-Richtlinie erstellen	Mittel	Gering	Intern koordiniert direkt mit SafeRoute	60 Tage

WIE WEITER?

Ihre nächsten Schritte.

1 **Standortbestimmung verstehen**

Wir besprechen die Standortbestimmung gemeinsam mit Ihnen. Dabei gehen wir sicher, dass die gesamte Standortbestimmung verstanden wurde.

2 **Angebot erarbeiten und vorstellen**

Bei Bedarf, erstellen wir sehr gerne ein Angebot für das Umsetzen der Massnahmen.

3 **Umsetzung starten**

Quick-Wins zuerst, danach die strategischen Themen. Wir begleiten Sie bei der Umsetzung der priorisierten Massnahmen und begleiten Sie kontinuierlich.

Sean Horvath
sean.horvath@saferoute.ch

DETAILANALYSEN

Anhang.

Detaillierte Bewertung aller fünf IKT-Bereiche mit Stärken, Handlungsbedarf und konkreten Themenscores. Ergänzt durch den technischen Aussenblick und die methodischen Grundlagen.

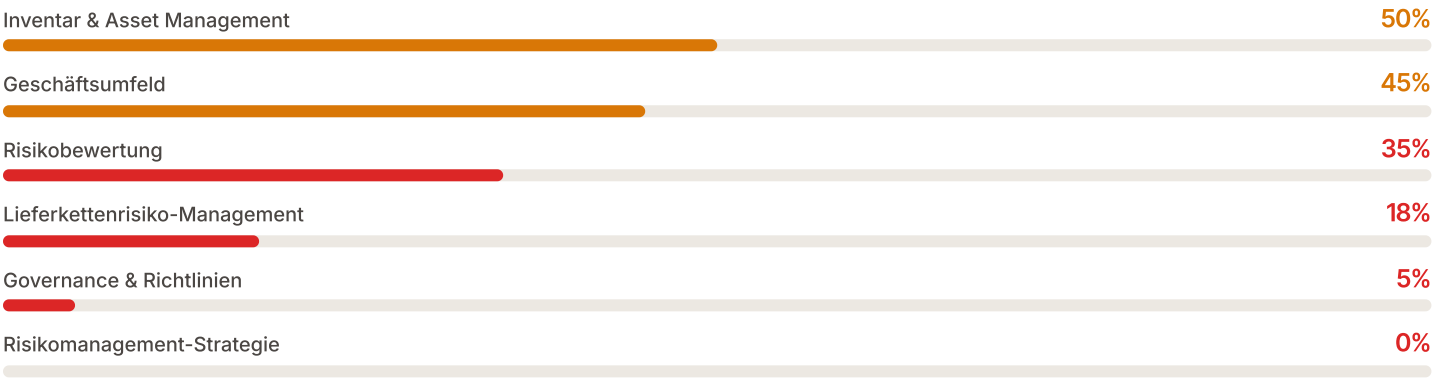
01 Identifizieren.

Verstehen Sie Ihre IT-Landschaft und Geschäftsprozesse. Dieser Bereich prüft, ob die Organisation ihre kritischen Vermögenswerte, Geschäftsprozesse und IT-Abhängigkeiten kennt und systematisch verwaltet.

25%
REIFEGRAD

Schwächster Bereich im Assessment. Die technische Landschaft ist gut bekannt (Inventar, Software), aber die strategischen Grundlagen fehlen. IT-Sicherheit wird operativ gut umgesetzt, ist aber noch nicht auf Ebene der Geschäftsleitung verankert.

6 THEMEN BEWERTET



STÄRKEN

- Hardware-Inventar vollständig und regelmässig aktualisiert.
- Eingesetzte Software und externe Systeme erfasst.
- Bei erkannten Risiken gibt es klare Reaktionspläne.
- Informationen über aktuelle Bedrohungen werden gesammelt.

HANDLUNGSBEDARF

- Keine dokumentierte Sicherheitsrichtlinie, keine definierten Rollen, keine Übersicht über gesetzliche Anforderungen.
- Risikomanagement-Strategie nicht vorhanden.
- Lieferantenrisiko wird nicht systematisch gesteuert. Kein SLA mit SwissIT Partner AG.
- Zulässige Ausfallzeiten für kritische Systeme nicht definiert.
- Organisatorische Kommunikationswege und Datenflüsse nicht dokumentiert.

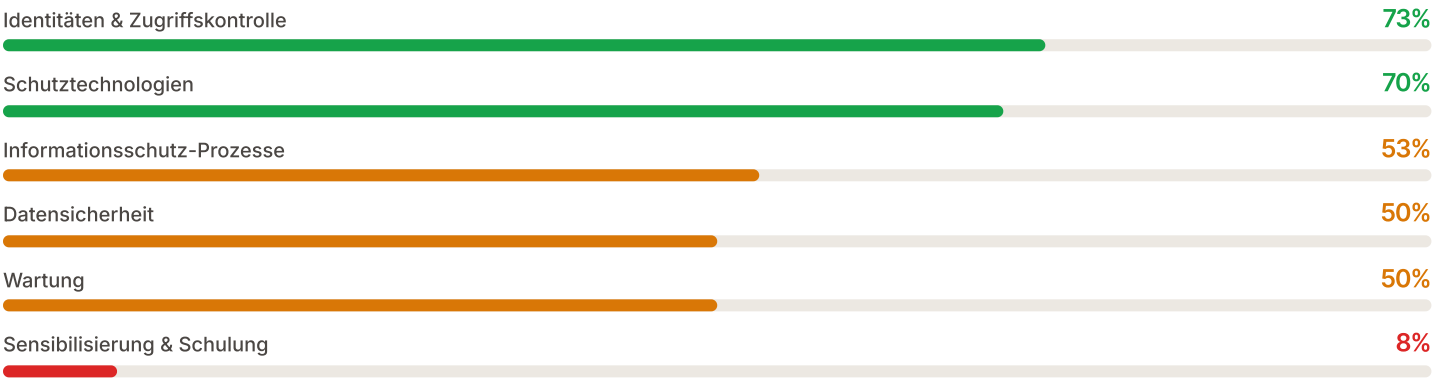
02 Schützen.

Setzen Sie technische und organisatorische Schutzmassnahmen um. Dieser Bereich bewertet die präventiven Schutzmassnahmen: Zugriffskontrolle, Datensicherheit, Schulungen und technische Schutzmechanismen.

50%
REIFEGRAD

Typisches Bild eines gut betreuten KMU: Die technischen Schutzmassnahmen sind durch SwissIT Partner AG solide umgesetzt. Der Handlungsbedarf liegt dort, wo Menschen und Prozesse ins Spiel kommen. Die Datensicherungsstrategie mit Veeam und Offsite-Kopie ist eines der stärksten Elemente im Assessment.

6 THEMEN BEWERTET



STÄRKEN

- Zugriffskontrolle solide: Prinzip der geringsten Rechte, eindeutige Zuordnung, zentrale Verwaltung.
- Datensicherung professionell: Veeam mit regelmässigen Tests, Offsite-Kopie auf dem NAS.
- Sichere Grundkonfiguration wird gepflegt und aktualisiert.
- Netzwerktrennung und Fernzugriffskontrolle funktionieren.
- Schutztechnologien solide: Crowdstrike, Mimecast, Barracuda Firewall.
- Test- und Produktivumgebungen getrennt.

HANDLUNGSBEDARF

- Schulung und Sensibilisierung deutlich unterentwickelt. Kein Schulungsprogramm.
- Physischer Zugangsschutz zum Serverraum nicht vorhanden.
- Kein Schutz gegen unkontrollierten Datenabfluss. Verschlüsselung nur teilweise.
- Sicherheitslücken werden nicht proaktiv gesucht.
- Gesetzliche Vorgaben (nDSG) werden nicht explizit überprüft.
- Wartungsarbeiten werden nicht dokumentiert.

03 Erkennen.

Überwachen Sie Ihre Systeme und erkennen Sie Anomalien. Dieser Bereich prüft, ob die Organisation Cyberangriffe und Anomalien zeitnah erkennen kann.

47%
REIFEGRAD

Zweigeteilte Realität: Was Crowdstrike und Mimecast automatisch abdecken, funktioniert zuverlässig. Darüber hinaus gibt es Lücken bei proaktiver Schwachstellensuche, physischem Monitoring und Überwachung externer Dienstleister.

3 THEMEN BEWERTET

Anomalien & Ereignisse — 55%

Kontinuierliche Überwachung — 48%

Erkennungsprozesse — 38%

STÄRKEN

- Netzwerküberwachung und Erkennung von Schadsoftware durch Crowdstrike zuverlässig.
- Sicherheitsereignisse werden analysiert und nach Wichtigkeit eingestuft.
- Auffällige Aktivitäten von Nutzern werden überwacht.
- Mimecast warnt aktiv bei verdächtigen Links in E-Mails.

HANDLUNGSBEDARF

- Schwachstellenanalysen werden nicht durchgeführt. Die externen Findings zeigen, was übersehen wird.
- Physische Umgebung wird nicht überwacht, kein Monitoring im Serverraum.
- Bei externen Dienstleistern werden Sicherheitsereignisse nicht überwacht.
- Erkennungssysteme werden nicht getestet.

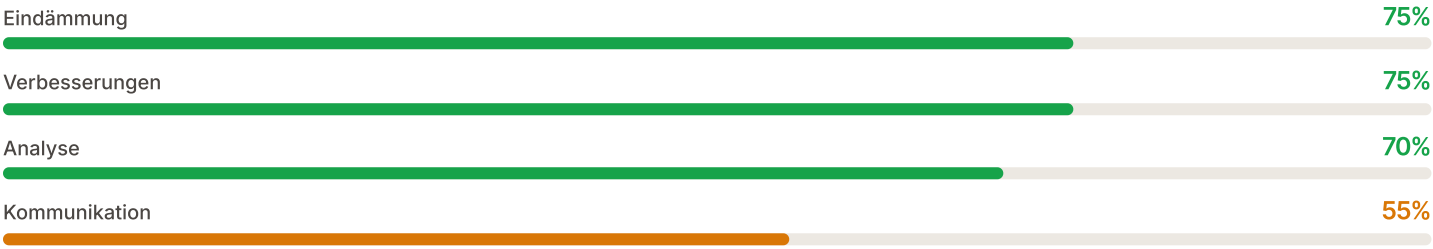
04 Reagieren.

Bereiten Sie sich auf IT-Notfälle und Sicherheitsvorfälle vor. Dieser Bereich bewertet, ob die Organisation auf erkannte Sicherheitsvorfälle strukturiert reagieren kann.

69%
REIFEGRAD

Stärkste Domäne. Die Kombination aus SwissIT Partner AG und Cyberversicherung bietet ein solides Sicherheitsnetz. Die Lücke liegt in der organisatorischen Verankerung: Der Notfallplan existiert technisch, ist aber im Unternehmen noch nicht breit bekannt.

4 THEMEN BEWERTET



STÄRKEN

- Eindämmung eingespielt: Isolation betroffener Systeme, Entfernung von Schadsoftware, Dokumentation.
- Forensische Untersuchung über Cyberversicherung abgedeckt.
- Vorfälle werden nach Schweregrad eingestuft und analysiert.
- Erkenntnisse fliessen in die Verbesserung der Pläne ein.
- Zusammenarbeit mit Strafverfolgungsbehörden geregelt.

HANDLUNGSBEDARF

- Notfallplan v0.2 existiert, ist aber organisatorisch nicht abgeschlossen.
- Mitarbeitende wissen nicht ausreichend über ihre Aufgaben bei einem Vorfall Bescheid.
- Der Notfallplan ist in der Organisation noch nicht ausreichend bekannt.

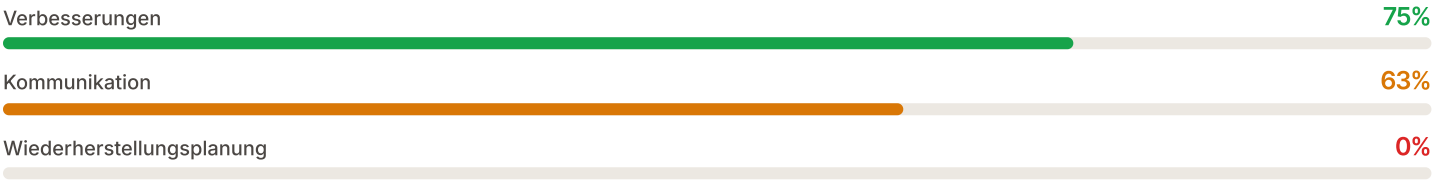
05 Wiederherstellen.

Stellen Sie den Betrieb nach einem Vorfall schnell wieder her. Dieser Bereich prüft, ob kritische Systeme und Prozesse nach einem Vorfall schnell und zuverlässig wiederhergestellt werden können.

46%
REIFEGRAD

Ordentliches Ergebnis, das differenziert betrachtet werden sollte. Die guten Werte kommen von Krisenkommunikation und Verbesserungsprozessen. Die eigentliche Wiederherstellungsplanung ist noch nicht formalisiert. Die technischen Mittel sind vorhanden, die geschäftliche Priorisierung steht noch aus.

3 THEMEN BEWERTET



STÄRKEN

- Krisenkommunikation über Cyberversicherung abgedeckt.
- Verbesserungsprozesse nach Vorfällen und Tests etabliert.
- Wiederherstellungsaktivitäten werden mit betroffenen Parteien kommuniziert.
- Kurze Entscheidungswege durch operativ tätige Inhaber.

HANDLUNGSBEDARF

- Wiederherstellungsplanung nicht formalisiert. Kein Plan mit Zeitzielen.
- Zulässige Ausfallzeiten pro System nicht festgelegt.
- Wiederherstellungsfähigkeiten auf Ebene der Geschäftsführung noch nicht transparent.

Analyse Ihrer öffentlich erreichbaren IT-Infrastruktur.

Eine externe technische Schwachstellenanalyse der öffentlich erreichbaren IT-Infrastruktur wurde durchgeführt. Die folgenden 14 Befunde wurden identifiziert und nach Kritikalität geordnet:

KRITISCH

5 BEFUNDE

MySQL-Datenbank offen aus dem Internet erreichbar

network

Auf dem Server 192.0.2.91 ist Port 3306 (MySQL) direkt aus dem Internet erreichbar. Das bedeutet, dass sich jeder weltweit mit der Datenbank verbinden und Login-Versuche starten kann. Automatisierte Werkzeuge scannen das Internet laufend nach genau solchen offenen Ports und probieren innerhalb von Minuten Standard-Passwörter und bekannte Kombinationen durch. Bei einem schwachen Passwort ist der vollständige Zugriff auf alle gespeicherten Daten möglich, inklusive Lesen, Verändern und Löschen.

EMPFOHLENE MASSNAHME

Port 3306 auf der Barracuda Firewall für eingehenden Traffic aus dem Internet sperren. Zugriff auf die Datenbank nur noch aus dem internen Netzwerk oder über VPN zulassen. Datenbankpasswörter erneuern.

Nginx 1.24.0 auf Abacus-Subdomains mit bekannten Sicherheitslücken

app

Die sieben Abacus-Subdomains (abacus, archiv, autodiscover, autodiscovery, kontakte, sync, voip) auf Port 9443 sowie der Server 192.0.2.146:9443 laufen mit Nginx 1.24.0 unter Windows. Diese Version ist von zwei dokumentierten Schwachstellen betroffen: CVE-2023-44487 (HTTP/2 Rapid Reset, ermöglicht Denial-of-Service-Angriffe) und CVE-2025-23419 (TLS Session Resumption, kann Zugriffsbeschränkungen umgehen). Beide Schwachstellen sind öffentlich dokumentiert und Angriffswerkzeuge sind frei verfügbar.

EMPFOHLENE MASSNAHME

Nginx auf den betroffenen Systemen auf die aktuelle stabile Version aktualisieren. Mit SwissIT Partner AG einen regelmässigen Patch-Zyklus für die Abacus-Infrastruktur vereinbaren.

Plesk 18.0.68 auf Webserver mit bekannter Sicherheitslücke

app

Der Webserver auf 192.0.2.91 (mueller-treuhand.ch) läuft mit Plesk Obsidian 18.0.68 Update 2, erreichbar über Port 8443. Diese Version ist von CVE-2025-66431 betroffen. Das Plesk-Login-Panel ist auf mehreren Domains und Subdomains öffentlich erreichbar, darunter mueller-treuhand.ch, shop.mueller-treuhand.ch, stage.mueller-treuhand.ch, staging.mueller-treuhand.ch und der Metanet-Server saphir.metanet.ch. Ein öffentlich erreichbares Admin-Panel mit einer bekannten Schwachstelle ist ein bevorzugtes Ziel für automatisierte Angriffe.

EMPFOHLENE MASSNAHME

Plesk auf die aktuelle Version aktualisieren. Mit Metanet als Hosting-Provider klären, ob das Update serverseitig durchgeführt wird. Zugang zum Plesk-Panel (Port 8443) auf bekannte IP-Adressen einschränken.

SSL-Zertifikat seit April 2023 abgelaufen auf 7 Subdomains

ssl_nested

Das SSL-Zertifikat für sieben Subdomains von mueller-treuhand.ch ist seit dem 26. April 2023 abgelaufen, also seit knapp drei Jahren. Betroffen sind die Subdomains abacus, archiv, autodiscover, autodiscovery, kontakte, sync und voip, jeweils auf Port 8443. Jede Verbindung zu diesen Diensten löst eine Sicherheitswarnung im Browser oder E-Mail-Client aus. Wenn Nutzer gewohnt sind, solche Warnungen wegzuklicken, werden sie auch bei einer echten Bedrohung nicht reagieren. Automatisierte Systeme und Integrationen können Verbindungen mit abgelaufenem Zertifikat komplett blockieren.

EMPFOHLENE MASSNAHME

Zertifikate für alle sieben Subdomains erneuern. Automatisierte Zertifikatsüberwachung einrichten, die mindestens 30 Tage vor Ablauf benachrichtigt. Prüfen ob Let's Encrypt für automatische Erneuerung eingesetzt werden kann.

TLS 1.0 aktiv auf Mail- und Webservern

ssl_nested

Auf beiden Müller AG-Servern wird das veraltete Verschlüsselungsprotokoll TLS 1.0 angeboten. Auf dem Mailserver 192.0.2.91 betrifft das die Ports 25 (SMTP), 587 (Submission), 465 (SMTPS), 993 (IMAPS), 995 (POP3S) sowie Port 8443 (Plesk). Auf dem zweiten Server 192.0.2.146 sind Port 444 und Port 9443 (Nginx/Abacus) betroffen. TLS 1.0 hat dokumentierte Schwachstellen (u.a. BEAST, POODLE) und wird von PCI DSS, NIST und dem BSI seit Jahren als unsicher eingestuft. Angreifer können die Schwachstellen nutzen, um verschlüsselten Datenverkehr mitzulesen.

EMPFOHLENE MASSNAHME

TLS 1.0 auf allen betroffenen Diensten deaktivieren. Nur noch TLS 1.2 und TLS 1.3 zulassen. Vorher prüfen, ob ältere Clients (z.B. alte E-Mail-Programme) betroffen wären.

HOCH

4 BEFUNDE

Veraltete CBC-Chiffren auf 8 Diensten aktiv

ssl_nested

Acht Dienste auf drei verschiedenen IP-Adressen bieten veraltete CBC-Chiffren (Cipher Block Chaining) an. Betroffen sind die Mimecast-Mailserver 194.104.108.22 und 194.104.110.22 (jeweils Port 587), der Abacus-Server 192.0.2.146 (Ports 444, 9443, 8443) sowie der Mailserver 192.0.2.91 (Ports 993, 995, 8443). CBC-Chiffren sind anfällig für Padding-Oracle-Angriffe und Timing-Angriffe, mit denen verschlüsselte Daten unter bestimmten Bedingungen entschlüsselt werden können.

EMPFOHLENE MASSNAHME

Veraltete CBC-Chiffren auf allen betroffenen Diensten deaktivieren. Stattdessen moderne AEAD-Cipher-Suites wie AES-128-GCM, AES-256-GCM oder ChaCha20-Poly1305 verwenden. Für die Mimecast-Server die Konfiguration über das Mimecast-Admin-Portal anpassen.

Keine starke Verschlüsselung auf SMTPS-Port

ssl_nested

Der SMTPS-Dienst auf 192.0.2.91:465 bietet keine Verschlüsselungsverfahren mit mehr als 128 Bit an und unterstützt kein Forward Secrecy. Forward Secrecy schützt vergangene Kommunikation auch dann, wenn der private Schlüssel des Servers zu einem späteren Zeitpunkt kompromittiert wird. Ohne Forward Secrecy könnte ein Angreifer, der den Schlüssel erlangt, nachträglich den gesamten aufgezeichneten E-Mail-Verkehr entschlüsseln.

EMPFOHLENE MASSNAHME

Cipher-Suite auf dem Mailserver aktualisieren: AES-256-GCM mit ECDHE (für Forward Secrecy) priorisieren. Schwache Cipher-Suites ohne Forward Secrecy entfernen.

Kein DMARC-Schutz für mueller-treuhand.ch

dns

Für die Domain mueller-treuhand.ch existiert kein DMARC-Record (_dmarc.mueller-treuhand.ch). DMARC definiert, was mit E-Mails passieren soll, die nicht von autorisierten Servern stammen: annehmen, in Quarantäne verschieben oder ablehnen. Ohne DMARC kann jeder im Internet E-Mails versenden, die aussehen als kämen sie von @mueller-treuhand.ch. Müller AG hat zudem keinen Einblick, ob jemand die Domain für gefälschte E-Mails missbraucht, weil ohne DMARC keine Aggregate-Reports generiert werden. Google und Microsoft setzen DMARC zunehmend voraus, E-Mails ohne DMARC-Schutz landen häufiger im Spam.

EMPFOHLENE MASSNAHME

DMARC-Record einrichten, zunächst im Monitor-Modus (p=none) mit Reporting-Adresse, um den legitimen Mailfluss zu analysieren. Nach Auswertung der Reports schrittweise auf p=quarantine und dann p=reject verschärfen.

Kein DKIM-Signing für mueller-treuhand.ch

dns

Für mueller-treuhand.ch sind keine DKIM-Selektoren konfiguriert (geprüft: selector1._domainkey, selector2._domainkey). DKIM signiert ausgehende E-Mails kryptographisch, sodass der Empfänger prüfen kann, ob die Nachricht unterwegs verändert wurde und tatsächlich vom angegebenen Server stammt. Ohne DKIM fehlt diese Integritätsprüfung. Zudem funktioniert DMARC-Alignment ohne DKIM nur über SPF, das aber bei Weiterleitungen regelmässig bricht. Mimecast als bestehender E-Mail-Provider unterstützt DKIM und kann die Signierung aktivieren.

EMPFOHLENE MASSNAHME

DKIM-Signing über die Mimecast-Administration aktivieren. DKIM-DNS-Records publizieren. Anschliessend zusammen mit DMARC in Betrieb nehmen.

MITTEL

3 BEFUNDE

Schwache Diffie-Hellman-Gruppe (512 Bit) auf Mailserver

ssl_nested

Die IMAP- und POP3-Dienste auf 192.0.2.91 (Ports 993 und 995) verwenden beim Schlüsselaustausch eine Diffie-Hellman-Gruppe mit nur 512 Bit. Das BSI empfiehlt mindestens 2048 Bit. Mit 512 Bit kann ein Angreifer mit moderater Rechenleistung den Schlüsselaustausch brechen und sich als Man-in-the-Middle in die Verbindung einklinken. Das betrifft den verschlüsselten E-Mail-Abruf der Müller AG-Mitarbeitenden.

EMPFOHLENE MASSNAHME

DH-Gruppe auf mindestens 2048 Bit umstellen. Idealerweise ECDHE (Elliptic Curve Diffie-Hellman) verwenden, das bei gleicher Sicherheit performanter ist.

3DES auf Abacus-Server aktiv

ssl_nested

Der Server 192.0.2.146 bietet auf Port 444 das veraltete Verschlüsselungsverfahren 3DES (Triple DES) an. 3DES hat eine effektive Blockgrösse von nur 64 Bit und ist anfällig für den Sweet32-Angriff, bei dem nach ca. 32 GB übertragener Daten Teile des Klartexts rekonstruiert werden können. Das Verfahren ist seit 2019 von NIST als veraltet eingestuft.

EMPFOHLENE MASSNAHME

3DES aus der Cipher-Suite-Konfiguration auf 192.0.2.146 entfernen. Stattdessen AES-GCM oder ChaCha20-Poly1305 verwenden.

Kein MTA-STS für mueller-treuhand.ch

dns

Für mueller-treuhand.ch existiert weder ein MTA-STS-Record (_mta-sts.mueller-treuhand.ch) noch eine MTA-STS-Policy. MTA-STS erzwingt, dass eingehende E-Mails nur über verschlüsselte Verbindungen (TLS) zugestellt werden. Ohne MTA-STS kann ein Angreifer im Netzwerk einen STARTTLS-Downgrade-Angriff durchführen: Er unterbindet die TLS-Verschlüsselung beim Mailempfang, sodass die E-Mail im Klartext übertragen wird und mitgelesen werden kann.

EMPFOHLENE MASSNAHME

MTA-STS-Policy als Textdatei unter https://mta-sts.mueller-treuhand.ch/.well-known/mta-sts.txt bereitstellen. Entsprechenden DNS-Record (_mta-sts.mueller-treuhand.ch) publizieren. Zunächst im Testing-Modus starten.

GERING

2 BEFUNDE

TLS 1.1 aktiv auf Mail- und Webservern

ssl_nested

Auf denselben Diensten wie TLS 1.0 wird auch TLS 1.1 angeboten: Mailserver 192.0.2.91 (Ports 25, 587, 465, 993, 995, 8443) und Abacus-Server 192.0.2.146 (Ports 444, 9443). TLS 1.1 ist zwar weniger kritisch als TLS 1.0, gilt aber seit 2021 ebenfalls als veraltet und wird von allen grossen Browsern und E-Mail-Clients nicht mehr unterstützt. Die Deaktivierung kann zusammen mit TLS 1.0 erfolgen.

EMPFOHLENE MASSNAHME

TLS 1.1 zusammen mit TLS 1.0 auf allen betroffenen Diensten deaktivieren. Nur TLS 1.2 und TLS 1.3 zulassen.

SPF-Record zu breit konfiguriert

dns

Der SPF-Record für mueller-treuhand.ch enthält neben den drei Include-Einträgen (scanscope.net, _spf.sui-inter.net, de._netblocks.mimecast.com) auch die Mechanismen +mx und +a. Damit wird dem Webserver (A-Record) und dem MX-Server erlaubt, E-Mails im Namen von mueller-treuhand.ch zu versenden. Falls der Webserver keine E-Mails versendet, erweitert +a die Autorisierung unnötig. Bei einer Kompromittierung des Webservers könnte ein Angreifer darüber legitim wirkende E-Mails im Namen von Müller AG versenden.

EMPFOHLENE MASSNAHME

SPF-Record bereinigen: +mx und +a entfernen, sofern der Webserver und MX-Server nicht aktiv E-Mails im Namen von mueller-treuhand.ch versenden. Die drei Include-Einträge (Mimecast, SUI, Scanscope) decken den legitimen Mailversand ab.

METHODIK

Grundlagen und Bewertungslogik.

Basis dieser Standortbestimmung:

Diese Standortbestimmung basiert auf dem IKT-Minimalstandard des Bundes, der seinerseits auf dem international anerkannten NIST Cybersecurity Framework aufbaut. Er umfasst 108 konkrete Massnahmen, verteilt auf fünf Funktionsbereiche — von der Identifikation kritischer Assets bis zur Wiederherstellung nach einem Vorfall.

FÜNF FUNKTIONSBEREICHE

1. Identifizieren
Vermögen Sie, Ihre kritischen Assets und Geschäftsprozesse?

2. Schützen
Sind präventive Schutzmassnahmen implementiert und gelebt?

3. Erkennen
Können Sie Cyberattacken zeitnah erkennen?

4. Reagieren
Existiert ein erprobter Incident-Response-Plan?

5. Wiederherstellen
Können kritische Systeme schnell wiederhergestellt werden?

REIFEGRADSKALA (0–4)

0	Unbekannt / Keine
1	Geplant / Ad hoc
2	Standardisiert
3	Integriert
4	Optimiert

Der Gesamtscore errechnet sich aus dem Durchschnitt aller bewerteten Massnahmen. Ein Zielwert von 65% (entspricht einem Reifegrad von 2.6/4) wird als angemessen für KMU erachtet.