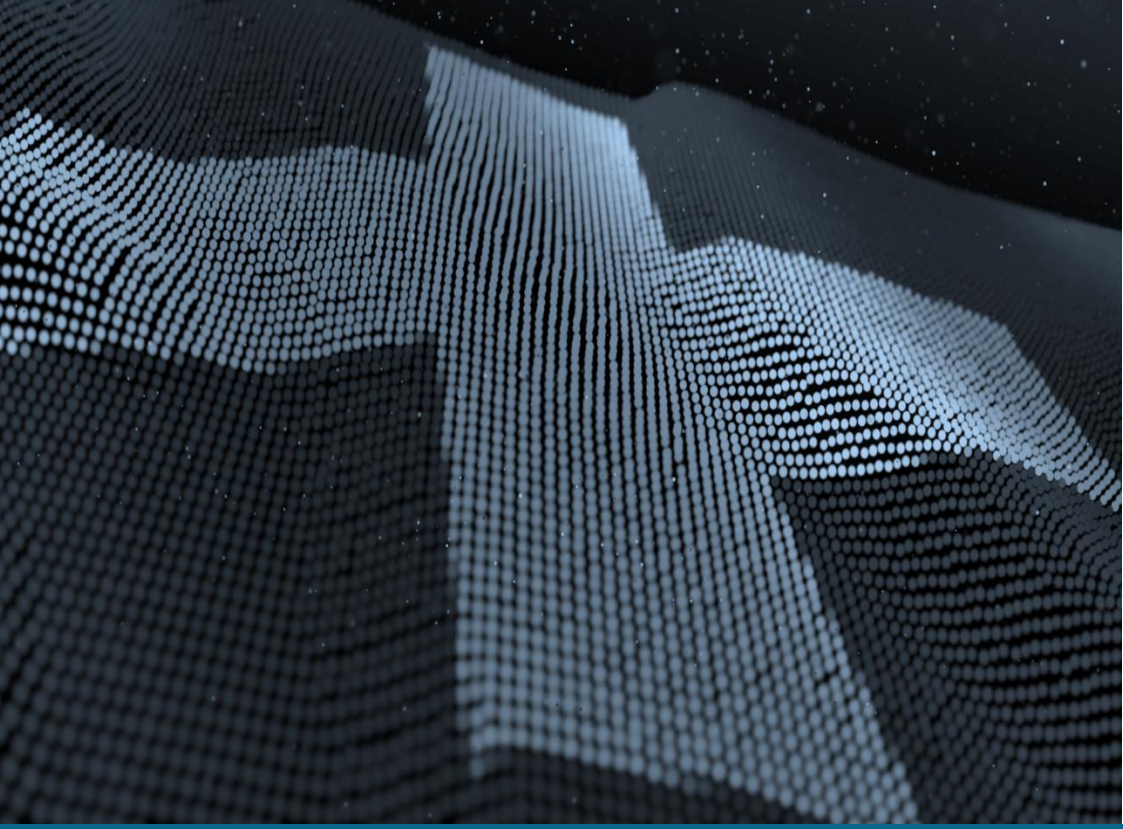

Ransomware
Schweiz

Unternehmen im Visier

asecus
securing your business

Abstract

Ransomware dominiert die Cyberbedrohungslandschaft weltweit. Auch in der Schweiz erfährt man über die Medien regelmässig über neue Fälle. Zu den Opfern zählen neben Unternehmen auch Gemeinden und Universitäten. Dieses Whitepaper untersucht relevante Studien zu Ransomware in der Schweiz, um einen Überblick über die Bedrohungslage hierzulande zu ermöglichen. Weiter wurden Erkenntnisse aus den Ransomware Readiness Checks (RRC), welche Asecus seit 2020 regelmässig durchführt, ausgewertet.

Die Studien kommen einheitlich zum Schluss, dass Ransomware sowohl in der breiten Bevölkerung als auch in den Führungsetagen als eine der Hauptbedrohungen wahrgenommen wird. Allerdings ist in vielen Unternehmen die Sicherheitsmaturität noch verbesserungswürdig. Ebenfalls konnten sowohl in den Studien als auch in den RRCs ein Wahrnehmungsunterschied zwischen Management, IT-Teams und den Mitarbeitern festgestellt werden. Es liegt an Führungskräften eine gelebte Sicherheitskultur zu etablieren und die involvierten Stakeholdern zu führen. Eines der Hauptprobleme ist das Fehlen einer holistischen Übersicht der Sicherheitsmaturität, was das effiziente Angehen von Verbesserungen hemmt.

Um nachhaltige Sicherheitsmassnahmen treffen zu können, sollten sich Führungskräfte sich so bald als möglich einen Gesamtüberblick über die Sicherheitslage in ihren Unternehmen verschaffen. Nur so kann sich ein Unternehmen langfristig vor der zunehmenden Bedrohung von Ransomware schützen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Einleitung

Ransomware ist eine der gefährlichsten Cyberbedrohungen für Unternehmen. Ein Fakt, welcher von unzähligen Security-Itelligence-Reports, aber auch durch medial präsente Fälle, unterstrichen wird. Unternehmen erkennen zwar die Gefahr von Ransomware, doch nur wenige ergreifen zusätzliche Massnahmen. Wie können Führungskräfte aktiv Einfluss auf den Schutz vor Ransomware nehmen? Dieses Whitepaper soll Führungspersonen einen Überblick über die aktuelle Ransomware-Lage in der Schweiz geben, Herausforderungen für die Unternehmensführung identifizieren und konkrete Schritte aufzeigen, wie die Unternehmensführung ihren Teil zum Schutz vor Cyberattacken beitragen kann.

Ransomware - Ein globales Phänomen

Ransomware ist eine Form von Malware, welche Opfer zum Zahlen einer Lösegeldsumme bewegen will. In der Regel geschieht dies durch Verschlüsslung von Daten und Systemen des Opfers. Oftmals steht bei einem Angriff die gesamte IT komplett still. Für Unternehmen ist ein solcher erfolgreicher Angriff mit sehr hohen Kosten verbunden. Es stellt sich die Frage, ob Lösegeld bezahlt werden soll und die nötigen Backups in akzeptabler Qualität verfügbar sind und eingespielt werden können. Auch verursachen die Downtime und die Bereinigung der Systeme erhebliche Kosten.

In jüngsten Fällen stehlen die Angreifer die Daten vorab, um ihre Opfer unter Androhung von Veröffentlichung zusätzlich unter Druck zu setzen. Man spricht auch von der Double Extortion Taktik. Mit der Triple Extortion werden zusätzlich auch noch Kunden und Partner des initialen Opfers bedroht. Etwa mit Androhung der Veröffentlichung sensitiven Informationen, welche auf den Systemen des ersten Opfers vorhanden sind, oder durch den Diebstahl von Zugangsdaten. Mit letzteren werden auch für sogenannte

Supplychain Attacken eingesetzt. Unternehmen, welche Dienste an andere Unternehmen ausgelagert haben, gaben damit auch ein Stück Kontrolle ab und haben so ihre Angriffsfläche erhöht.

Ablauf eines Ransomware-Angriffs

Der Ablauf eines Ransomware Angriffs lässt sich vereinfacht in drei Phasen unterteilen. Abbildung 1 zeigt einen grafischen Ablauf. Als erstes verschaffen sich die Angreifer initialen Zugriff zum Unternehmensnetzwerk. Dazu nutzen sie unter anderem Phishing, um an gültige Zugangsdaten zu geraten oder versuchen mit Bruteforce in Services einzudringen. Mit diesen können sie sich dann im Opfernetzwerk anmelden. Phishing wird aber auch verwendet, um Nutzer zum Öffnen von maliziösen Dokumenten (meistens Excel oder Word) zu bewegen, um so Malware auf ein Zielsystem zu installieren. Angreifer nutzen aber auch bekannte Schwachstellen in Software aus, um sich so Zugriff zu einem System zu verschaffen. Letzteres kann automatisiert werden und verursacht für Angreifer minimalen Aufwand.

Ist die initiale Malware erst einmal auf einem Zielsystem installiert, meldet sich diese bei sogenannten Command and Control Servern, um weiter Instruktionen zu erhalten. In dieser Phase werden zum Beispiel weitere Komponenten nachgeladen. Ebenfalls versuchen die Angreifer, sich im Unternehmensnetzwerk auszubreiten (Lateral Movement) und höhere Rechte zu erlangen (Privilege Escalation). Das Endziel der Angreifer ist in der Regel ein Domain-Admin Account. So können Angreifer das gesamte Unternehmensnetzwerk kontrollieren.

Haben die Angreifer das Netzwerk unter ihre Kontrolle gebracht beginnen sie mit den eigentlichen Aktionen. Sie stehlen sensitive Daten, verschlüsseln alle Computer im Netzwerk inklusive der Backups. Den Opfern wird dann auf den Desktops in der Regel das

Erpresserschreiben mit den Instruktionen zur Zahlung angezeigt. Einige Ransomware Gangs bieten sogar eine Supporthotline an, welche die Opfer etwa beim Kauf von Crypto-Währungen unterstützt.

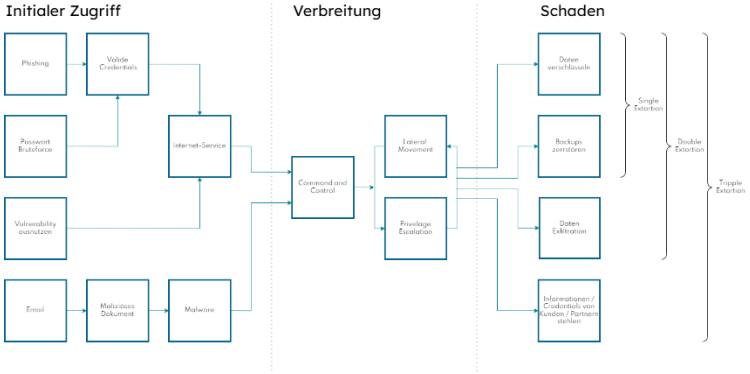

Abbildung 1: Vereinfachter Ablauf einer Ransomware Attacke

Der Schaden für Unternehmen ist dabei erheblich: Durch die Verschlüsselung aller IT-Mittel wird ein Unternehmen von einem Tag auf den anderen komplett handlungsunfähig. Es können keine Aufträge erfasst werden, keine Services und Produktion erbracht werden. Es werden sensitive Unternehmensdaten oder datenschutzrelevante Informationen gestohlen. Es fallen Kosten für die Systemreinigung und Wiederherstellung und allfällige Lösegeldzahlungen an. Ferner können etwa durch Verfahren eingeleitet durch Kunden, Partner oder staatliche Organe Rechtskosten anfallen und es droht ein Reputationsschaden für das Unternehmen.

Ransomware in der Schweiz

Auch in der Schweiz nehmen Ransomware Angriffe zu. Das Nationale Zentrum für Cybersicherheit (NCSC) warnt bereits seit 2019 Unternehmen nachdrücklich vor solchen Angriffen. [1]. Das NCSC

spricht Ransomware das höchste Schadenspotential zu. Von 2020 zu 2021 haben sich die Meldungen beim NCSC zu Ransomware mehr als verdoppelt [2]. Diese Entwicklung widerspiegelt sich auch in der medialen Berichterstattung. In jüngster Vergangenheit kam es zu mehreren medial publik gewordenen Ransomware Angriffen. Neben Unternehmen fielen auch Gemeindeverwaltungen und Universitäten bereits zum Opfer von Ransomware.

Die Security Branche nimmt die Zunahme von Ransomware mit Ernüchterung zur Kenntnis. Im "The State Ransomware 2021 Report" von Sophos wurden unter anderem auch Schweizer Unternehmen befragt. Dabei gaben 46% der Schweizer Unternehmen an, im letzten Jahr von Ransomware betroffen gewesen zu sein. Damit belegt die Schweiz den achten Platz nach Indien, Österreich, USA, Israel, Türkei, Schweden und Belgien. Global beträgt der Durchschnitt 37%. Gemäss dem Report betragen die global durchschnittlichen Behebungskosten einer Ransomware Attacke 1.85 Millionen US-Dollar. Dabei werden Downtime, Arbeitszeit, Gerätekosten, Netzwerkkosten, Lösegeldsummen und Verluste durch verlorene Aufträge berücksichtigt. In der Schweiz sind die Kosten mit 1.43 Millionen US-Dollar leicht unter dem Durchschnitt und belegen somit Platz 12 [3].

Neues DSG - Neue Pflichten

Die Schweiz erhält ein neues Datenschutzgesetz (DSG). Aufgrund der rasanten technologischen Veränderungen ist das aktuelle Datenschutzgesetz nicht mehr zeitgemäss und erhält eine Totalrevision. Das neue Gesetz soll gemäss aktuellen Aussagen des Bundesamts für Justiz per 1. September 2023 in Kraft treten. Zusätzlich wird mit der Totalrevision das Ratifizieren des revidierten Datenschutzübereinkommens des Europarates und relevante Schengen Richtlinien ermöglicht werden.

Mit der Revision kommen wesentliche Neuerungen auf Unternehmen zu. Etwa die Erarbeitung oder Anpassung der Datenschutzerklärung und die Etablierung von Prozessen wie der Auskunftsprozess. Weiter kommt mit dem neuen DSG auch eine Meldepflicht bei Datenschutzverletzungen und Sanktionen von bis zu 250'000 CHF [4]. Im Hinblick auf Ransomware dürfte vor allem die Meldepflicht Unternehmen wesentlich tangieren, da bei einem erfolgreichen Ransomware-Angriff datenschutzrelevante Einsichten durch Unberechtigte erfolgen.

Ransomware Studien

Das Thema Ransomware ist sowohl in der breiten Bevölkerung als auch in den Chefetagen ein bekanntes Thema. Doch die Meinungen gehen auseinander, wie damit umgegangen werden soll. Dieser Abschnitt fasst relevante Umfragen und Studien kurz zusammen und ordnet sie ein.

In der breiten Bevölkerung wächst die Sorge vor Cyberangriffen: Die Jahresstudie „Sicherheit" von der Militärakademie, ETH Zürich, und dem Center for Security Studies befragte Schweizerinnen und Schweizer zur Ermittlung langfristiger Trends in aussen-, sicherheits- und verteidigungspolitischen Meinungen. Die Bedrohung der Datensicherheit wird als die höchste Gefahr wahrgenommen, auch wenn in jüngster Zeit eine leichte Abnahme erkennbar ist. 2021 fühlen sich 28% sehr oder eher bedroht. Die Eintrittswahrscheinlichkeit eines Cyberangriffs wird von den Befragten als zweithöchste Gefahr eingeschätzt (49% sehr oder eher wahrscheinlich). Nur die Gefahr durch eine globale Pandemie wird höher bewertet. Diese erhielt im aktuellen Bericht, aufgrund der Covid-19 Pandemie, eine massiv höhere Gewichtung als noch vor ein paar Jahren [5].

Cyberbedrohungen werden auch in Schweizer Führungsetagen zunehmend diskutiert. Im CEO Survey von PWC aus 2021 bekundeten 93% Besorgnis über Cyberattacken. Damit liegt die Schweiz leicht über dem globalen Durchschnitt. Jedoch gaben nur 46% der befragten Geschäftsführer an, dass ihre Organisation mehr Massnahmen ergreifen sollte (Welt 36%). Auch wurde die Frage, ob die Organisation aufgrund der Covid-19 Pandemie mehr Langzeitinvestitionen im Bereich Cyber tätigen wolle, von nur 77% bejaht. PWC hielt im Bericht fest, dass diese Zahl aufgrund der aktuellen Sicherheitsmaturität deutlich näher bei 100% liegen sollte. Auch Reporting war ein Teil der Befragung. Ein Viertel der CEOs gaben an, mehr Reporting im Bereich Datenschutz und Cybersicherheit einzuführen [5].

Die Einschätzungen der CEOs stehen jedoch im Kontrast zu den Meinungen von Mitarbeitern. In der CISCO Cybersecurity Umfrage 2021, an welcher auch 251 Schweizer teilnahmen, gaben 36% der Befragten an, dass ihr Unternehmen Security nicht ernst genug nehme. Fast die Hälfte der Befragten fühlt sich bezüglich IT-Sicherheit bei ihrem Arbeitgeber nicht gut aufgehoben und wünschen sich explizit mehr Initiative. Es fehle an Awareness: Fast ein Viertel, nämlich 23%, gaben an noch nie eine Sicherheitsschulung erhalten zu haben. Besonders im Bereich Homeoffice, welches aufgrund der Covid-19 Pandemie in vielen Unternehmen in kurzer Zeit flächendeckend ausgerollt wurde, besteht erheblicher Nachholbedarf: Gerade mal 53% der Befragten nutzen einen VPN-Client und nur 45% haben die Multifaktor Authentifizierung aktiviert. 15% der Befragten gaben an, nichts über Sicherheitstechnologien im Homeoffice zu wissen oder keinen Zugang darauf zu haben. wieter gaben 42% der Befragten an, bestehende Sicherheitstechnologien zu umgehen. Angesichts der zunehmenden Angriffen auf Schweizer Unternehmen überrascht das Ergebnis. Das Unsicherheitsgefühl von Mitarbeitern und das Umgehen von Sicherheitstechnologien

zeige, dass es an gelebten Sicherheitskulturen fehlt. Neben technischer Aufrüstung besteht auch hier erheblicher Aufholbedarf in Unternehmen [6].

Auch HP Wolf Security untersuchte die Auswirkungen der Pandemie auf das Verhältnis zwischen Angestellten und Security Experten. In dieser Studie gaben 31% der Befragten an Sicherheitsmechanismen zu umgehen. IT-Teams drückten ihren Fraust aus, dass die Sicherheit im Homeoffice eine zweitrangige Rolle spielte und sie sich durch die Geschäftsleitung unter Druck gesetzt fühlten. 83% der befragten IT-Fachkräfte gaben an, dass die wachsende Zahl von Mitarbeitern im Homeoffice eine tickende Zeitbombe sei. Als Massnahme schränkten viele IT-Teams den Zugang zu Daten und Systemen stark ein, was sie in den Augen der Mitarbeiter als Bösewicht erschienen liess. So gaben 80% der befragten IT-Teams an, dass die IT-Sicherheit zu einer undankbaren Aufgabe geworden sei. Die Autoren der Studie warnen vor einer Eskalation der Spannungen und Risiken, wenn das Management nicht eingreift [7].

Es scheint einen Unterschied in der Wahrnehmung zwischen Management, IT-Teams und Mitarbeitern zu geben. Dieser Wahrnehmungsunterschied wurde anfangs 2022 hervorgehoben: Das GovCERT forderte auf dem Postweg 130 Schweizer Organisationen auf, darunter auch Gemeinden, ihre Systeme zu patchen. Abbildung 2 zeigt den Tweet des GovCERT. Vorgängige Aufforderungen per Mail seien ignoriert worden. Es fehlt also nicht nur an technischen, sondern auch an organisatorischen Massnahmen in Unternehmen, um einen angemessenen Schutz gegen Ransomware zu gewährleisten. Es liegt an den Führungskräften, die Kluft zwischen den IT-Mitarbeitern, dem Management und den Mitarbeitern zu überwinden und eine gelebte Sicherheitskultur in Unternehmen zu etablieren.

Abbildung 2: Tweet GovCERT.ch

Feld-Erfahrungen Asecus

Die Asecus AG führt seit zwei Jahren Ransomware Readiness Checks (RRC) in Unternehmen durch. In Interviews wird die gesamte Organisation auf ihre Sicherheits-Maturität untersucht. Dabei werden neben den technischen Massnahmen auch organisatorische Abläufe und Prozesse untersucht. Regelmässig stellt sich heraus, dass kein Gesamtüberblick vorhanden ist. Dies erschwert zum einen das produktive Arbeiten, aber auch nachhaltige Investitionen in die Sicherheitsinfrastruktur werden dadurch gehemmt. Unternehmen gehen Probleme oftmals nur selektiv an, obwohl zwischen unterschiedlichen Problemen Synergien in den Lösungen

genutzt werden können, was Kosteneinsparungen und effizientere Problembehebung ermöglicht. Abbildung 3 zeigt die Verteilung der Ergebnisse in den einzelnen Phasen eines Ransomware Angriffs mit einem Score zwischen 0 und 5.

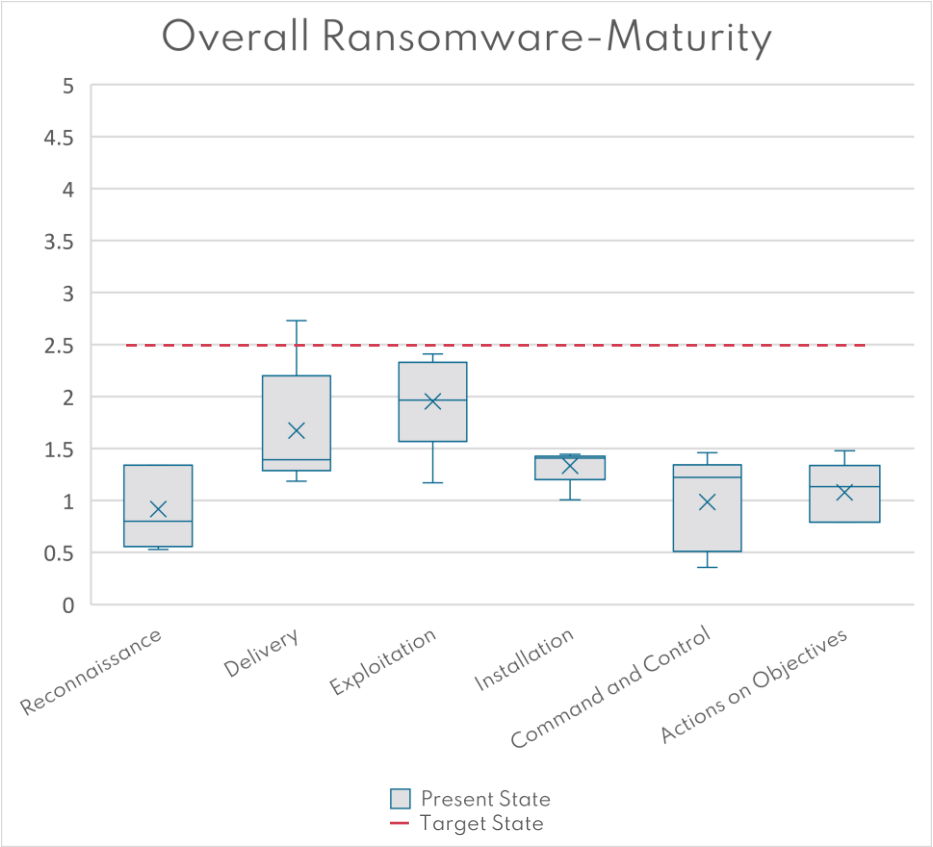

Abbildung 3: Verteilung der Ergebnisse RRCs

In allen Phasen befinden sich die meisten Unternehmen deutlich unter dem erwünschten Target State von 2.5. Nur im Bereich Delivery gab es vereinzelte Unternehmen, welche den Target State übertrafen. Am besten, aber immer noch ungenügend, aufgestellt sind

die Unternehmen in den Bereichen Delivery und Exploitation. Im Bereich Delivery konnte Asecus erkennen, dass viele Firmen einen Prozess eingerichtet haben, um Phishing-E-Mails zu melden. Ebenfalls erfreulich ist, dass diese Unternehmen mittels E-Mail Security-Lösungen das Risiko eines Ransomware-Befalls deutlich reduzieren konnten. Auch wenn der Einsatz dieser Massnahmen bei allen untersuchten Unternehmen besser sein könnte, besteht vor allem im Bereich der Handhabung von BYOD oder USB-Sticks und Remote Access enormes Verbesserungspotential.

Im Bereich Exploitation konnte Asecus bei den untersuchten Unternehmen den Einsatz einer Endpoint Protection (EPP) Lösung und ein akzeptables Patch Management feststellen. Auch in diesen Bereichen gibt es für alle Unternehmen noch Verbesserungspotential, wie zum Beispiel das Einsetzen einer EPP Lösung für Linux Server oder das genauere Definieren der Prozesse und Verantwortlichkeiten beim Patch Management. Weitere Verbesserungspunkte sind überwiegend im Bereich des System-Hardenings anzusiedeln.

In den Interviews mit den Unternehmen konnte Asecus regelmässig feststellen, dass der Wahrnehmungsunterschied zwischen den bereits erwähnten Stakeholdern besteht. Viele Unternehmen haben vor allem in organisatorischen Bereichen erheblichen Nachholbedarf. Insbesondere im Hinblick auf das neue DSG sind Unternehmen in der Pflicht, neue Prozesse und Rollen innerhalb der Organisation zu schaffen.

Eine Führungsherausforderung

Ransomware ist ein komplexes Problem. Es umfasst unterschiedliche technische Aspekte wie Netzwerksicherheit, Endpoint Protection, Rechtvergabe, aber auch organisatorische Massnahmen wie das Etablieren einer Security Kultur, regelmässiges Schulen der

Mitarbeiter und Implementierung von Incident- und Recovery-Prozessen.

Weiter wird das Problem durch eine nicht unbeachtliche Anzahl an Stakeholdern verstärkt. Besonders für KMU stellt sich die zusätzliche Herausforderung der Ressourcenknappheit. Die meisten KMU verfügen über keinen Chief Information Security Officer (CISO) oder Security Teams. Diese Rollen werden im Extremfall von nur einer Person getragen. Damit wird eine seriöse Abdeckung aller Aspekte verunmöglicht. Etwa durch fehlendes Know-How oder mangelnde Zeit, um diesen Tätigkeiten in angemessenem Umfang nachzugehen. Doch wie sollten Führungspersonen vorgehen, um die IT-Security in ihrem Unternehmen Nachhaltig zu verbessern?

1. Überblick Verschaffen
2. Handlungsfelder identifizieren
3. Verantwortlichkeiten und Timelines definieren
4. Kontrollieren

In den meisten Unternehmen fehlt es heute an einer holistischen Übersicht über die Schutzmassnahmen. Die Informationen sind verteilt in verschiedenen Zuständigkeitsbereichen oder gar nicht erst vorhanden. Ohne eine Übersicht über die aktuelle Maturität der IT-Security, können Massnahmen nicht effizient eingeführt werden. Aus diesem Grund sollten Unternehmen als erstes einen Status Quo erheben und Handlungsfelder identifizieren.

Sind die Handlungsfelder aufgedeckt, können die Führungspersonen zusammen mit ihren IT-Teams oder externen Partnern Lösungen finden, welche das Bedürfnis zu akzeptablen Kosten und Aufwand abdecken. Vielleicht gibt es Synergien, welche genutzt werden können, um mehrere Aspekte mit einer Lösung abzudecken.

Definieren Sie die Projekte mit Scope, Verantwortlichkeiten und Timelines und stellen Sie den Projektfortschritt in regelmässigen Meetings fest, um frühzeitig auf Probleme reagieren zu können.

Cybersecurity ist kein einmaliger Event, sondern ein stetiger Prozess. Bedrohungen ändern sich laufend. Darauf müssen Unternehmen reagieren können. Folgende Prozesse oder Tätigkeiten sollten Führungskräfte regelmässig durchführen und kontrollieren:

Patchmanagement: Es muss sichergestellt werden, dass Softwareupdates regelmässig und zeitnah installiert werden, besonders kritische Sicherheitsupdates. Definieren Sie Zuständigkeiten für Systeme, damit eine Accountability gewährleistet ist und sich die zuständigen Personen verantwortlich fühlen. Richten Sie sich ein Dashboard ein, um den Status zu überwachen. Ein regelmässiger Vulnerability Scan ichn als zusätzliches Kontrollinstrument dienen.

Mitarbeiterschulungen: Führen Sie regelmässig Mitarbeiter Schulungen durch, in welchen Sie aktuelle Bedrohungen und Gefahren vermitteln. Auch sollten Sicherheitsrichtlinien regelmässig mittgeteiicherden, dass sich Mitarbeitende über ihre Pflichten im Klaren sind und interne Prozesse wie der Incident-Prozess klar und verständlich kommunichrt werden. Führen Sie Lernkontrollen durch, um den Wissenstand zu messen und Schulungsunterlagen zu verbessern.

Recovery-Prozesse: Die meisten Unternehmen verfügen heute über Backupprozesse undichpeichern ihre relevanten Daten regelmässig. Was jedoch in den meisten Unternehmen noch nicht durchgeführt wird, ist regelmässiges Üben von Daten und Systemwiederherstellungen. Zum einen können dadurch die technische Integrität der Daten überprüft werden, aber auch der organisatorische

Ablauf. Weiter können IT-Teams durch regelmässiges Üben ihre Reaktionszeiten im Ernstfall verkürzen.

Diese Prozesse müssen gelebt werden. Führungskräfte sollten deshalb als Vorbild auftreten und die Wichtigkeit durch Sinnvermittlung allen Mitarbeitern weitergeben. Holen Sie sich regelmässiges Feedback sowohl von IT-Teams als auch Mitarbeitern ein, um Bedenken und Unklarheiten frühzeitig abzufangen und darauf eingehen zu können. Für eine gelebte Sicherheitskultur in Unternehmen könnten auch Incentive-Modelle überlegt werden. Beispielsweise das Belohnen von Mitarbeitern, welche Phishing-Mails melden. Bereits ein schön formuliertes Dankesmail motiviert Mitarbeitende, auch in Zukunft das Richtige zu tun und die Unternehmung vor Cyberbedrohungen zu bewahren.

Schlusswort

Ransomware ist und bleibt eine der gefährlichsten Bedrohungen für Unternehmen. Das Problem wurde in den meisten Chefetagen erkannt, jedoch ist die Behebung der aktuellen Missstände alles andere als trivial. Wir hoffen, Ihnen einen Überblick über Ransomware in der Schweiz und Ihnen als Führungsperson Anhaltspunkte für mögliche erste Schritte zur Verbesserung Ihrer Security-Posture ermöglicht zu haben. Die Asecus AG ist seit 1997 als Security Dienstleister tätig und betreut heute über 200 Kunden in unterschiedlichen Branchen und Standorten. Seit 2020 betreuen wir unsere Kunden mit dem Ransomware Readiness Check. Dieser ist interviewbasiert und soll vor allem Führungskräften und IT-Teams eine Übersicht und gemeinsame Diskussionsgrundlage bieten. In den Interviews gehen wir auf jede Phase eines Ransomware Angriffs ein und beleuchten sowohl technische als auch organisatorische Bereiche. Die Ergebnisse werden grafisch aufgearbeitet, um eine gute Übersicht über das aktuelle Sicherheitslevel im

Unternehmen zu schaffen und wir geben Ihnen konkrete Handlungsempfehlungen, welche Sie treffen können, um Ihr Sicherheitsniveau zu erhöhen.

Quellenverzeichnis

[1] Nationales Zentrum für Cybersicherheit, „Verschlüsselungstrojaner greifen vermehrt gezielt Unternehmensnetzwerke an," 9 Mai 2019. [Online]. Available: Verschlüsselungstrojaner greifen vermehrt gezielt Unternehmensnetzwerke an.

[2] Nationales Zentrum für Cybersicherheit, „Wochenrückblick 52," 4 Januar 2022. [Online]. Available: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/wochenrueckblick_52.html.

[3] Sophos, „The State of Ransomware," Sophos , Abingdon, 2021.

[4] Bundesamt für Justiz, „Stärkung des Datenschutzes," 2022. [Online]. Available: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html.

[5] T. S. Tresch, A. Wenger, S. De Rosa, T. Ferst, C. Gloor und R. Jacques, „Sicherheit 2021 - Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend," Militärakademie (MILAK) an der ETH Zürich und Center for Security, Birmensdorf und Zürich, 2021.

[6] PwC, „CEO Survey 2021," PwC, London, 2021.

[7] R. Jaun, „Schweizer Mitarbeitende kritisieren die Cybersecurity ihrer Unternehmen," netzwoche, Zürich, 2021.

[8] R. Koller, „Darum kriselt es zwischen dem Security-Team und Mitarbeitenden im Homeoffice," netzwoche, Zürich, 2021.

[9] M. Stockley, „A doctor reveals the human cost of the HSE ransomware attack," Malwarebytes Labs, Santa Clara, 2021.

[10] B. O'Donovan, „HSE cyber-attack cost hits €43m, could rise to €100m," RTÉ, Dublin, 2021.

Asecus AG
Undermülistrasse 24
8320 Fehraltorf
info@asecus.ch

asecus
securing your business