ALARM
Awareness Labor KMU Informationssicherheit

Niederschwelliges Sicherheitskonzept zum Thema Schutzmaßnahmen BestPractice

für Geschäftsführung und IT-Verantwortliche

Thinking Objects GmbH

Stand: August 2023

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Das vorliegende **niederschwellige Sicherheitskonzept für KMU** ist eines von insgesamt sieben Sicherheitskonzepten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der Technischen Hochschule (TH) Wildau verfasst werden.

Das Projekt „ALARM Informationssicherheit“ wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Das niederschwellige Sicherheitskonzept für KMU basiert auf Ergebnissen der im Projekt „ALARM Informationssicherheit“ durch den Unterauftragnehmer Thinking Objects (TO) GmbH in Pilotunternehmen durchgeführten „Vor-Ort-Angriffen“.

Das diesem Sicherheitskonzept zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

1 Einleitung 3

1.1 Risiko-Bewertung 4

1.2 Was kann ich selbst leisten? 4

2 Schutzmaßnahmen 4

2.1 Zugriffe aus dem Internet 5

2.2 Berechtigungs-Management 5

2.3 Antivirus 5

2.3 Antivirus 5

2.4 Backup und Recovery 6

2.5 Updates & Patch-Management 6

2.6 Unternehmens-Netzwerk 6

2.7 Internet-Anbindung 7

2.8 Redundanz 7

1 Einleitung

In diesem Sicherheitskonzept soll versucht werden, eine Blaupause zu beschreiben, um Anforderungen an die Technik im Sinne der IT-Sicherheit korrekt umzusetzen.

IT-Infrastruktur und IT-Sicherheit sind keine unbedeutenden Kostenfaktoren, so dass in der Regel nicht alle möglichen Maßnahmen umgesetzt werden können. Leider wird im Rahmen der Kosten für Funktionalität der IT-Infrastruktur dann auch oft die IT-Sicherheit vernachlässigt. Das können sowohl notwenige Produkte zum Schutz und zur Detektion sein als auch notwendigen Aufwände zur korrekten Implementierung.

Aber beide Komponenten der IT-Systemlandschaft haben relevante Auswirkungen auf das Business-Continuity-Management, kurz BCM, für ein Unternehmen. Dieses liegt in der Verantwortung der Unternehmensleitung und damit ist auch IT-Sicherheit ein Thema, dass die Unternehmensleitung selbst vorleben und treiben muss und nicht auf die IT-Leitung abwälzen kann.

1.1 Risiko-Bewertung

Auch in einem kleinen Unternehmen ist es wichtig, eine vereinfachte Risiko-Bewertung zu machen. Diese kann in tabellarische Form erfolgen.

Hier müssen alle relevanten Systeme aufgelistet sein. Zu jedem der Systeme müssen Sie sich überlegen, wie wichtig es für die zentrale Wertschöpfung ist. Für die kurzfristigen Auswirkungen stellt sich die Frage, wann der Ausfall eines Systems zu einem Stillstand der Produktion oder des Verkaufs oder weiterer zentraler Geschäftsprozesse führt.

Zusätzlich zum Ausfall eines Systems sollte das zweite Szenario eines Datenverlustes in diesem System bewertet werden. Hierbei können Sie sowohl einen Datenverlust zur letzten Woche, zum letzten Monatsersten oder auch einen vollständigen Datenverlust in Betracht ziehen.

Systeme, die üblicherweise in jedem Unternehmen existieren und eine Relevanz für die zentrale Wertschöpfung haben, sind in der Regel die Kommunikations-Systeme (E-Mail, Telefonie) und ERP mit Modulen wie Buchhaltung, Warenwirtschaft, CRM, Außendienst, Projektcontrolling, oder auch E-Commerce. Zusätzlich kommen noch Infrastruktur-Systeme wie Netzwerk, Firewalls, Internet-Anbindung und Virtualisierungsumgebung hinzu.

Wenn Sie beim Ausfall zentraler Systeme die meisten ihrer Beschäftigten für den Rest des Tages, der Woche oder des Monats nach Hause schicken müssen, können Sie den möglichen Schaden für das Unternehmen abschätzen und auch die möglichen Investitionen in IT-Infrastruktur und IT-Sicherheit beziffern.

1.2 Was kann ich selbst leisten?

Für ein mittelständisches Unternehmen ist die Fokussierung auf die eigentliche Wertschöpfung notwendig. IT ist in der Regel nur ein unterstützender Prozess. Im Rahmen der aktuellen Situation mit einem Fachkräftemangel muss sich auch die IT auf die Aufgaben spezialisieren, die entsprechend zentral für das Unternehmen sind: Hierzu kommen oftmals der Helpdesk und Endanwender-Support sowie die Anpassung der ERP-Systeme. Die übrigen Tätigkeiten können an Dienstleister und Managed Service Provider vergeben werden. Hier können beispielsweise auch Aufgaben wie regelmäßiges Patchen von Servern und Clients erbracht werden, oder auch der Betrieb der Virtualisierungsumgebung. Auch die Pflege der Firewall oder des Internet-Zugriffs kann hier an spezialisierte Dienstleister vergeben werden.

Enthalten die eigenen Produkte allerdings Software-Komponenten, greifen andere Regeln. Diese würden den Rahmen dieses Sicherheitskonzeptes allerdings überschreiten.

2 Schutzmaßnahmen

Es gibt ein paar technische Grundprinzipien, mit denen Systeme und Daten heute abgesichert werden müssen.

Für ein kleines oder mittelständisches Unternehmen empfehlen wir den Einsatz eines Herstellers im Umfeld der IT-Security. Die großen Unternehmen können es sich leisten, die sogenannten „Best of Breed“-Lösungen einzusetzen und diese miteinander zu integrieren. Für ein kleines Unternehmen empfiehlt sich der Einsatz der Suite eines Her-

stellers, die beispielweise Komponenten wie Firewall, Surf-Schutz und Endpoint-Protection miteinander integriert und über eine zentrale Plattform auswerten und betreiben lässt.

2.1 Zugriffe aus dem Internet

Alle Zugriffe die direkt aus dem Internet auf Unternehmensdaten oder Systeme möglich sind, müssen mit einem sogenannten zweiten Faktor abgesichert werden. Der Einsatz von Login und Passwort reicht hier nicht aus.

Das betrifft beispielsweise Zugriffe mittels VPN auf das Unternehmens-Netzwerk aus dem Internet, oder auch die Nutzung von virtuellen Arbeitsplätzen aus dem Internet. Internet bedeutet hier sowohl das Home-Office als auch das Internet-Café oder das Gäste-WLAN beim Kunden/Partner oder auch die Mobil-Funk-Verbindung der eigenen Laptops oder Smartphones.

Auch der Zugriff auf Dokumente und Daten in Cloud-Systemen, die aus dieser Sicht schon im Internet liegen, müssen durch einen zweiten Faktor geschützt werden. Nicht diskutieren wollen wir hier den datenschutzrechtlichen Aspekt, ob die Daten an den entsprechenden Dienstleister oder Service übergeben werden dürfen. Das betrifft E-Mail-Systeme genauso wie etwaige Cloud-basierten Datenspeicher. Bei jedem professionellen Anbieter werden Zwei-Faktor oder Multifaktor-Lösungen angeboten.

Aber auch wenn die E-Mails nicht in der Cloud, sondern in Unternehmensnetzwerk liegen, darf der Zugriff aus dem Internet nicht ohne zweiten Faktor erfolgen. Das betrifft sowohl Web-Zugriff als auch Client-Zugriff oder auch den Zugriff mit dem Smartphone. Für letzteres existieren spezielle Mobile-Device-Management-Systeme die den zweiten Faktor über eine technische Lösung und strenge Kontrolle des Endgerätes sicherstellen.

2.2 Berechtigungs-Management

Da so gut wie jedes Unternehmen heute Windows-Rechner und ein Active Directory einsetzt, haben sich Hacker genau auf diese Umgebung spezialisiert. Wer die Kontrolle über das Active Directory erlangt, hat die Kontrolle über die gesamte integrierte Umgebung, das ist das Ziel der Angreifer. Daher ist es wichtig, speziell die administrativen und privilegierten Benutzer und Accounts besonders zu schützen. Für die Administration müssen die normalen Accounts klar von den Admin-Accounts getrennt sein. Kein Account darf lokal administrative Rechte haben, denn hier können Angreifer mit der Erkundung und Übernahme entsprechend starten. Die Kontrolle der existierenden privilegierten Accounts muss auch regelmäßig erfolgen, damit beispielsweise von Angreifern angelegte Hintertüren entsprechend erkannt werden.

2.3 Antivirus

Ein Antivirus-Programm alleine ist heute nicht mehr ausreichend. Die Hersteller professioneller Lösungen integrieren den Antiviren-Schutz heute mit weiteren Mechanismen, um speziell die Sicherheit und Vertrauenswürdigkeit eines Arbeitsplatzes sicherzustellen. Diese sogenannten Endpoint Protection-Systeme sichern einen Arbeitsplatz, beispielsweise ein Laptop, auch zusätzlich ab, wenn er sich außerhalb des Unternehmensnetzwerkes befindet. Dort wo keine Unternehmens-Firewall den Zugriff auf das Internet reguliert, kann die Endpoint-Protection-Lösung weiterhin Zugriffe auf gefährliche Internet-Seiten unterbinden.

2.4 Backup und Recovery

Zentraler Bestandteil jedes Notfall- und Wiederherstellungskonzeptes ist die Backup-Strategie. Hiermit müssen sowohl Elementar- und Naturereignisse als auch Hackerangriffe mit Ransomware abgewehrt werden. Für ersteres benötige ich eine Auslagerung (und Verschlüsselung) außerhalb eines bestimmten Umkreises. Für das zweite muss ich sicherstellen, dass bei Kompromittierung meines Unternehmensnetzwerkes die Backup-Umgebung und die Sicherungsdaten unangreifbar und unzerstörbar bleiben. Als Faustregel gilt hier, das Backup immer unabhängig vom Active Directory aufzubauen sowie eine externe Auslagerung beispielsweise auf Bändern durchzuführen. Es besteht immer das Risiko, wenn sich ein Angreifer lange im Netzwerk bewegt, auch diese Schutzmechanismen auszuhebeln.

Alle Daten bei Cloud-Anbietern sind in der Regel von Cloud-Betreiber nicht gesichert, sondern werden nur redundant vorgehalten. Das leitet sich aus der gemeinsamen und geteilten Verantwortung ab, die sich aus dem Service-Vertrag ergibt.

Darum müssen auch Daten in der Cloud ebenfalls in ein Unternehmens-Backup integriert werden. Für viele weit verbreitete Services liefern aktuelle Backup-Programme die entsprechenden Schnittstellen auch mit. Für manche Cloud-Services entstehen hier allerdings zusätzliche Kosten durch Benutzung einer Schnittstelle oder die übertragenen Datenmengen.

2.5 Updates & Patch-Management

Fehlende Updates sind ein hohes Risiko für alle Systeme, speziell für die direkt mit dem Internet verbundenen. Allerdings können auch schlecht gewartete Systeme im Unternehmensnetzwerk Eindringlingen die Ausbreitung im Netz ermöglichen.

Patch-Management ist der Vorgang, die Updates aller Systeme nicht dem Zufall zu überlassen. Hierbei müssen alle Systeme berücksichtigt werden: Arbeitsplätze, Laptops, Tablets, Smartphones, Server, Switches, Router, Firewalls, Steuergeräte und auch Drucker und Kopierer.

Für die windows-basierten Serversysteme und auch die Windows-Arbeitsplätze gibt es Software, sogenannte Patch-Management-Software, die bei der Verteilung von Updates, sowohl für das Betriebssystem aber auch für die Applikationen unterstützt.

Für alle anderen Arbeitsplatz-Systeme mit Betriebssystemen wie Linux oder MacOS muss ebenfalls sichergestellt werden, dass sie in einem unternehmensweiten Patch-Management integriert sind.

2.6 Unternehmens-Netzwerk

Das Unternehmensnetzwerk muss segmentiert sein. Das bedeutet, dass Arbeitsplätze und Clients, Server, Drucker und Produktionsmaschinen in unterschiedlichen Netzbereichen sind, die nur über die Firewall miteinander kommunizieren können. Auf diesen Weg kann man unterschiedlich kritische Systeme voneinander trennen und dafür sorgen, dass Angreifer sich nicht mehr frei im internen Netz bewegen können, wenn sie einen Arbeitsplatz erfolgreich übernommen haben.

Auch für Systeme, die keine Updates mehr bekommen, ist eine Isolation im Netzwerk der einzige Weg, den Rest der IT vor Sicherheitsrisiken durch diese Systeme zu schützen. Das betrifft oftmals die Steuerung von Produktions-Maschinen, kann aber auch das alte Buchhaltungssystem betreffen, dass nur noch zum Nachschauen oder eine

mögliche Steuerprüfung vorgehalten wird.

2.7 Internet-Anbindung

Die Internet-Anbindung erfährt beispielsweise durch die Nutzung von Cloud-Systemen oder Web-Portalen für verschiedenste Anwendungen eine immer höhere Wichtigkeit in der täglichen Bearbeitung. Auch diese Dienste können in der Risiko-Bewertung aufgeführt werden. Wenn keine Versandaufträge mehr erstellt werden können, ist vielleicht das Auslieferungslager innerhalb weniger Stunden überfüllt und sorgt auf diesem Weg für Probleme.

Somit gibt es auch für die Internet-Leitung eine entsprechende Wichtigkeit für die üblichen Betriebsprozesse festzulegen. Durch heutige Firewalls und SD-WAN-Technologien benötigt man in der Regel keine Leitung mit eingebautem Backup durch den Carrier mehr, sondern kann zwei unabhängig Leitungen nutzen. Einzige Ausnahme hierfür ist das Angebot von Webservices am Standort, hier kann es dennoch notwendig sein, einen IP-Bereich redundant anzubinden.

2.8 Redundanz

Redundanz erhöht in der Regel die Verfügbarkeit der Services. Der Schwerpunkt sollte hierbei auf die kritischen Services gelegt werden, wie sie in der Risiko-Klassifizierung festgelegt wurden. Welcher Ausfall kompensiert werden kann und muss ist entsprechend festzulegen.

Existiert eine interne Virtualisierungsumgebung, sollte diese im normalen Tagesbetrieb einen Virtualisierungshost als Reserve haben, um den Ausfall eines Knoten weitgehend zu kompensieren.

Werden zwei Serverräume betrieben, sollte sichergestellt werden, dass die Infrastruktur eines Serverraums ausreicht, um den Betrieb des Unternehmens zu gewährleisten. Hiervon sind somit nicht nur Systeme sondern auch die Daten betroffen.

Die Redundanz der Internet-Anbindung wurde im entsprechenden Kapitel schon beschrieben.

Technische Hochschule Wildau
Technical University of Applied Sciences

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770400
Fax. +49 711 88770449
www.to.com