Arvato Systems Whitepaper

Das nächste Level von digitaler Security am Arbeitsplatz

Ihr Leitfaden für eine zuverlässige Sicherheitsstrategie im Digital Workplace

ARVATO SYSTEMS

START

Einleitung: Cyber-Angriffe bedrohen die Existenz von Unternehmen

Gefahrenquelle für die digitale Sicherheit

- Remote Work: Cloud-Arbeitsplätze führen zu neuem Angriffsraum
- Social Engineering: Mitarbeitende als Türöffner für Cyberkriminelle
- Klassische Angriffsmethoden

Herausforderungen im modernen Cyber War

Step by Step zu professioneller Cyber Security

- Schritt 1: Dokumentation der Ist-Situation
- Schritt 2: Definition des Soll-Zustands
- Schritt 3: Optionen erörtern und planen
- Schritt 4: Einführung der neuen Strategie
- Schritt 5: Laufender Betrieb

Microsoft 365 Defender und Microsoft Defender for Cloud für den Schutz von Unternehmensdaten

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Defender for Identity und Azure AD Identity Protection

Managed Microsoft Security Services

Fazit

CYBER-ANGRIFFE BEDROHEN DIE EXISTENZ VON UNTERNEHMEN

Cyber-Angriffe können jedes Unternehmen treffen – ob Großkonzern oder Kleinunternehmen, die Gefahr lauert heutzutage überall. Insbesondere in Zeiten von digitalen Arbeitsplätzen nutzen Kriminelle die Angriffsfläche von Cloud-Systemen, um in Netzwerke einzudringen, Daten zu stehlen und Schaden anzurichten. Die Auswirkungen sind starke Beeinträchtigungen im Arbeitsablauf, bis hin zur Insolvenz von Unternehmen und der Arbeitslosigkeit von Mitarbeitenden.

Dazu kommt der Schaden durch verlorene Daten von Kund:innen und Lieferunternehmen, die ebenfalls unverschuldet durch erfolgreiche Angriffe beeinträchtigt werden. „Die Wucht, mit der Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Unternehmen aller Branchen und Größen“, kommentiert Bitkom-Präsident Achim Berg die aktuelle Entwicklung.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt in seinem Lagebericht zur IT-Sicherheit in Deutschland 2021 vor einer stark wachsenden Zahl von Angriffen auf die IT-Infrastruktur von Unternehmen und Organisationen. Allein die Masse an neuen Schadprogrammen hat im Jahr 2021 um rund 144 Millionen zugenommen. Das sind knapp 394.000 neue Malware-Programme pro Tag. Im Vergleich zum Vorjahr beträgt das Wachstum noch einmal knapp ein Viertel.

In diesem Whitepaper erläutern wir Ihnen die Gefahren von unzureichender Sicherheit im Digital Workplace und stellen Lösungen vor, um die Herausforderungen erfolgreich zu meistern. Wir zeigen nachfolgend, wie zuverlässige Sicherheitssysteme Cyber-Attacken erkennen, verhindern und somit Unternehmensdaten schützen.

GEFAHRENQUELLEN FÜR DIGITALE DATEN

Cyberkriminelle haben heutzutage zahlreiche Mittel und Wege, Angriffe auf Unternehmen durchzuführen. Dabei spielt der Digital Workplace eine große Rolle – Systeme, die sich außerhalb des Unternehmensnetzwerks befinden, bieten prinzipiell eine größere Angriffsfläche. Diese Fläche muss durch eine strategische und ganzheitliche Cyber Security minimiert werden. Wir stellen Ihnen verbreitete Einfallstore für Angreifende im digitalen Arbeitsumfeld vor. Berücksichtigen Sie diese, erreichen Sie ein höheres Cyber Security Level als im Classic Workplace.

Remote Work: Cloud-Arbeitsplätze führen zu neuem Angriffsraum

Neben der Arbeit an den physischen Unternehmensstandorten arbeiten immer mehr Anwendende auch mobil und im Home Office. Im Digital Workplace arbeiten Nutzende von überall, in verschiedenen Netzwerken, mobil, zu Hause und auch cloudbasiert. Die vielfältigen Möglichkeiten für effektives Arbeiten öffnen gleichzeitig Angriffsflächen für Kriminelle, denn in Cloud-Systemen ist der Schutz nach außen nicht mehr ausreichend. Cyberkriminelle bahnen sich den Weg in Ihr Unternehmensnetzwerk, um gezielt von innen anzugreifen. Verantwortliche müssen daher aktiv gegensteuern und den Schutz der digitalen Arbeitsplätze von innen heraus sicherstellen.

Ohne aktive Sicherheitsmaßnahmen ist die Gefahr von Angriffen im Home Office und beim mobilen Arbeiten natürlich besonders groß. Bereits ein einzelner erfolgreicher Angriff auf einen Heimarbeitsplatz kann zu ungeahnten Schäden im Unternehmen führen. Nach einer repräsentativen Bitkom-Studie aus dem Jahr 2021 geben über die Hälfte der Unternehmen an, dass IT-Sicherheitsvorfälle vor allem auf die Arbeit im Home Office zurückzuführen sind.

Social Engineering: Mitarbeitende als Türöffner für Cyberkriminelle

Cyber-Attacken resultieren in zahlreichen Sicherheitsvorfällen – angefangen bei erfolgreicher Verschlüsselung der Unternehmensdaten durch Ransomware bis zur anschließenden Erpressung der Unternehmen für die Freigabe der Daten. Das BSI warnt dazu: „Angreifer nutzen auch verstärkt den Faktor „Mensch“ als Einfallstor für Angriffe, die mit Social-Engineering-Methoden arbeiten und gleichsam als Türöffner für weitere Angriffe dienen“.

Laut der Bitkom-Studie sind über 40 Prozent der befragten Unternehmen von Cyber-Angriffen betroffen, bei denen Kriminelle Beschäftigte manipulieren. Davon fällt allein fast ein Viertel auf E-Mail-Systeme. Social Engineering, also der Versuch der Manipulation von Mitarbeitenden, ist bei den veränderten Arbeitsbedingungen und beim Einsatz des Digital Workplace ein riesiges Einfallstor für Kriminelle.

In der Regel zielen Cyberkriminelle auf den Diebstahl von Daten, Erpressung von Lösegeld oder Industriespionage. Den Angreifenden geht es also um Geld, wie einem Wirtschaftsunternehmen auch. Der Diebstahl umfasst von Kommunikations- und Kundendaten über sensible Finanzinformationen bis hin zu kompletten Zugangsdaten für Cloud-Dienste alles, was über kriminelle Methoden zu Geld gemacht werden kann. Sind der Aufwand und die Kosten für die Hacker:innen zu hoch, lohnt sich ein Angriff aus wirtschaftlicher Sicht jedoch nicht mehr. Ziel ist es also, die Hürden so hochzusetzen, dass der monetäre Zweck eines Angriffs seinen Sinn verliert.

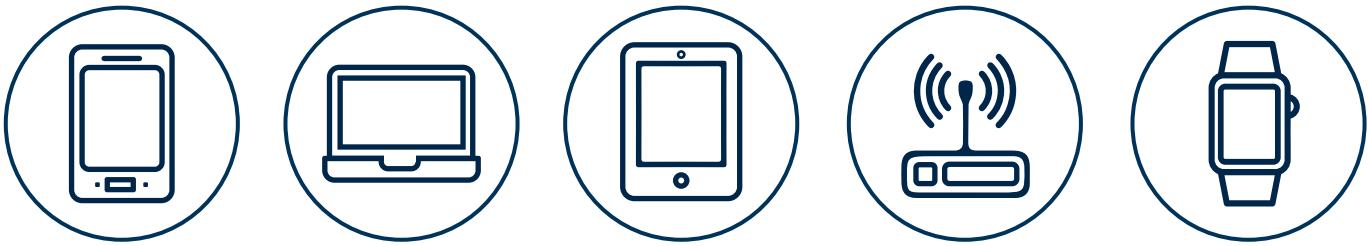
Klassische Angriffsmethoden

Auch altbekannte Angriffsmethoden wie das Vortäuschen von falschen Identitäten (Spoofing), das Abfangen von sensiblen Daten (Phishing), Social Engineering oder herkömmliche Malware kommen nicht weniger häufig vor. Bei einem Drittel der Unternehmen verursachte Malware erheblichen Schaden. Bei ebenfalls einem Drittel wurden Ressourcen gezielt durch Angreifende überlastet, sodass Mitarbeitende, die Kund:innen und Lieferunternehmen diese nicht mehr nutzen konnten.

Solche Distributed Denial of Service Angriffe, kurz DDoS-Angriffe, sind seit Jahren bekannt und steigen jährlich an, zuletzt um 10 Prozent von 2019 auf 2020. Im August 2021 hat Microsoft den bisher größten DDoS-Angriff von 70.000 Rechnern auf seine Azure-Cloud abgewehrt – übrigens auch mit Tools, die wir in diesem Whitepaper vorstellen. Der Angriff fand darüber hinaus über PCs statt, auf denen Malware aktiv war. Die Anwendenden wussten davon in den meisten Fällen nichts. Auch das lässt sich durch Tools verhindern, die wir Ihnen vorstellen.

HERAUSFORDERUNGEN IM MODERNEN CYBER WAR

Die einfache Installation von Virenscannern und Firewalls reicht für den Schutz von Netzwerken bei Weitem nicht mehr aus. Die Angriffsmuster von Cyberkriminellen haben sich verändert und verändern sich täglich. Unternehmen müssen sich auf diese neuen Angriffsmuster vorbereiten und anpassen. Viren sind keine einfachen Programme mehr, sondern intelligente Softwares, die Dateien verschlüsseln, Daten stehlen, Endgeräte sperren oder die komplette Kontrolle übernehmen. Nicht nur stationäre PCs sind gefährdet, Schadprogramme greifen auch andere Endgeräte an. Dabei verstecken sich Kriminelle in Netzwerken, greifen Zugangsdaten ab und führen den Angriff im Namen der anwendenden Person durch. Gefährdet sind unter anderem:



Smartphones Laptops Tablets Heimnetzwerke Smartwatches

Auch Cryptojacking ist ein häufiger Angriff, bei dem Kriminelle nahezu die gesamte Leistung von PCs nutzen, um Kryptowährungen zu erstellen. Das kostet Energie und Rechenleistung, die den Anwendenden für die Arbeit nicht mehr zur Verfügung steht. Dazu kommt die Übernahme von Rechnern zu Bot-Netzwerken, mit denen Kriminelle wiederum Angriffe starten.

Die permanente Bewegung in der Bedrohungslandschaft kann für Sicherheitsverantwortliche frustrierend sein. Aber: Mit der Verlagerung von Arbeitsplätzen in die Cloud öffnen sich nicht nur zahlreiche Türen und Wege für Kriminelle. Cloud Systeme bieten auch neue Möglichkeiten und Chancen für die Cyber Security. Das Security-Level, das Cloud-Systeme erreichen können, könnten herkömmliche On-Premises-Lösungen niemals abbilden.

STEP BY STEP ZU PROFESSIONELLER CYBER SECURITY

Außer Frage steht, dass jedes Unternehmen sich mit dem Thema Cyber Security befassen muss. Wie aber sichere ich nun meine moderne, digitale Arbeitsumgebung im dynamischen Cyber War?

Eine rundum zuverlässige und sichere Strategie für Cyber Security ist mindestens so facettenreich und komplex, wie sie für die Sicherheit Ihrer Unternehmensdaten essenziell ist. Damit Sie den Überblick bei der Absicherung Ihrer digitalen Arbeitsplätze bewahren, spielt eine strukturierte Vorgehensweise eine wichtige Rolle. Wir haben Ihnen die wichtigsten Schritte auf dem Weg zu Ihrer Cyber Security-Strategie zusammengefasst.

Schritt 1: Dokumentation des Ist-Zustandes

Im ersten Schritt der Planung steht die Aufnahme der Ist-Situation. Die Projektverantwortlichen sollten sich darüber im Klaren sein, welche Tools und Dienste das Unternehmen bereits nutzt. Ein genauer Blick lohnt sich: Oftmals taucht im Rahmen einer Ist-Analyse bislang unbekannte Schatten-IT auf, die ebenfalls sicherheitsrelevant ist. Auch die Prozessabläufe, Aufgaben und alle Aktivitäten rund um die bestehende Cyber Security gehören in die Ist-Aufnahme. An dieser Stelle steht ebenfalls die Erfassung der vorhandenen Kapazitäten für Advanced Security – sowohl auf quantitativer als auch auf qualitativer Ebene. Der Ist-Zustand identifiziert gegebenenfalls bereits Schwachstellen und Gefahrenzonen mit erhöhtem Sicherheitsrisiko.

Haben Sie ausreichend Ressourcen zur Hand, können Sie in der Theorie eine Sicherheitsstrategie eigenständig intern umsetzen. Da ein Außenstehender aber oftmals einen neutraleren Blick auf die Situation werfen kann und darüber hinaus über fachspezifisches Wissen verfügt, ist es in jedem Fall empfehlenswert, auf externe Services zurückzugreifen – in welchem Umfang Sie diese nutzen, ist individuell von Ihrem Bedarf abhängig. Erwägen Sie, Teile des Projekts auszulagern oder mit einem Partner durchzuführen, können Sie bei einigen Anbietern bereits im ersten Schritt auf die Unterstützung zählen.

Schritt 2: Definition des Soll-Zustands

Sobald der Ist-Zustand dokumentiert ist, geht es an die Definition des gewünschten Soll-Zustands. Dieser Schritt setzt die Projektziele fest und steckt somit einen Rahmen für die Vorgehensweise ab. Wichtige Aspekte für die Definition des Soll-Zustands sind das gewünschte Sicherheitslevel, das die Cyber Security-Strategie sicherstellen soll und darüber hinaus der Umfang und die Art der Systeme sowie die dazugehörigen Prozesse, die die Strategie abdecken soll.

Schritt 3: Optionen erörtern und planen

Im nächsten Schritt steht ein Brainstorming für die benötigten Tools, Anwendungen, Dienste, Prozesse und Skills an. Welche Möglichkeiten bietet der Markt? Welcher Weg ist für die Sicherheit meiner digitalen Arbeitsplätze am besten? Spätestens an diesem Punkt tritt die Frage auf, ob das Projekt Inhouse durchgeführt werden soll oder ob ein externer Dienstleister eine sinnvolle Ergänzung für die eigene Cyber Security-Strategie ist. Sie definieren, gemeinsam mit einem Partner oder allein, auf welche Lösungen und Vorgehensweisen Sie in Zukunft für die Sicherheit Ihrer Netzwerke, digitalen Arbeitsplätze und Identitäten zurückgreifen möchten. Sie möchten mehr darüber erfahren, wie Sie IT-Sicherheit als Business-Prozess etablieren können? In unserem Blogartikel erfahren Sie alles über das Management von Cyber Security.

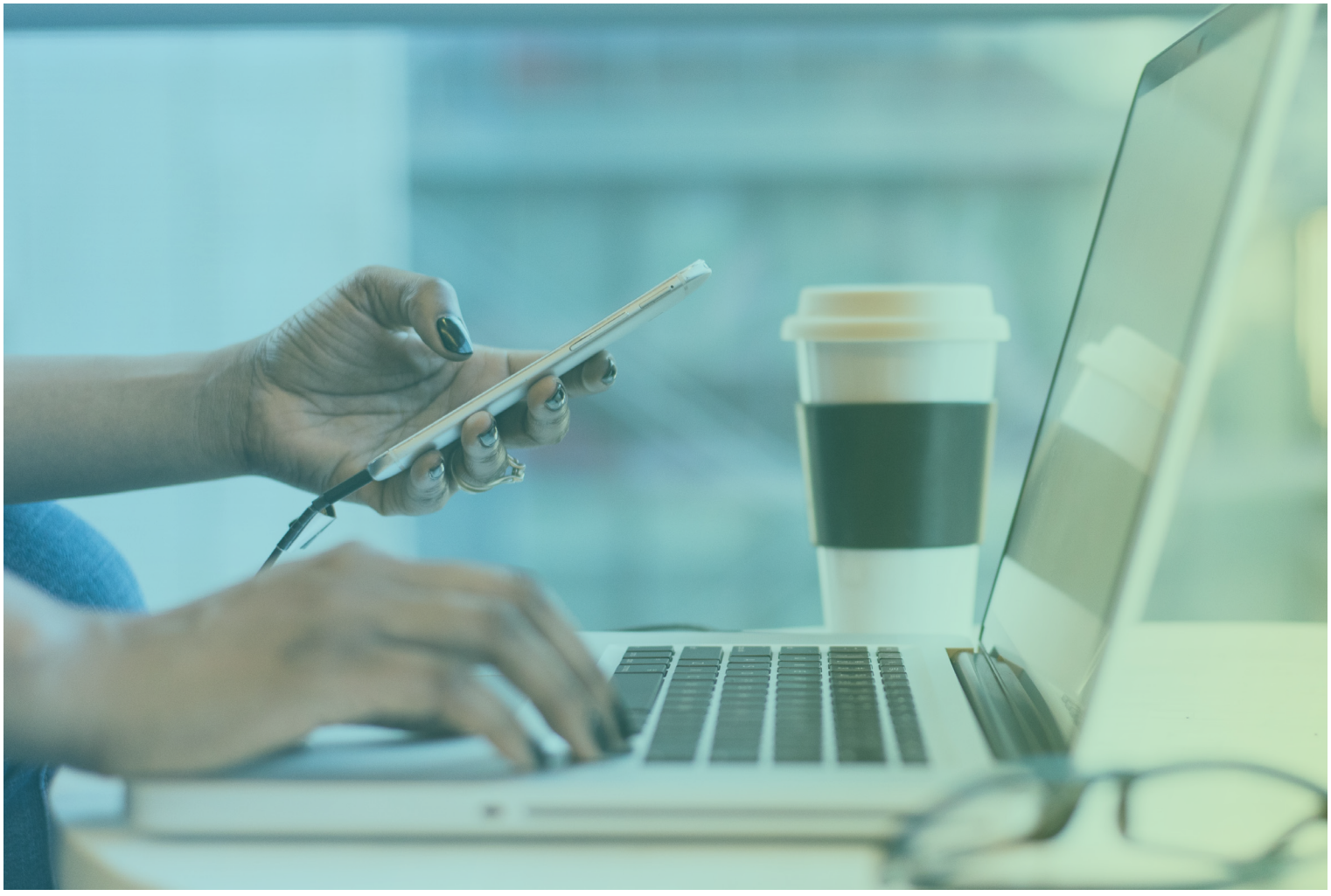
Schritt 4: Einführung der neuen Strategie

Die nächsten Schritte beinhalten die Umsetzung der geplanten Schritte. Dazu gehören die Einführung und Konfiguration der Tools und Anwendungen sowie die Etablierung der dazugehörigen Prozesse. Die genaue Vorgehensweise ist natürlich davon abhängig welche Dienste, Tools und Aktivitäten in der individuellen Strategie eine Rolle spielen. Dafür sollten Sie sich mit Ihrem Security Operations Center (SOC) abstimmen, das bereits ab der Auswahl und Konfiguration Ihrer Tools für alle Aktivitäten im Rahmen Ihrer Sicherheitsstrategie zuständig ist. Wichtig ist, dass nicht nur die technische Implementierung hierbei berücksichtigt werden darf. Jedes Tool, jeder Service und jede Anwendung ist nur hilfreich, wenn es auch genutzt wird – berücksichtigen Sie also über den gesamten Verlauf das Changemanagement, um durch Verständnis und Wissen eine hohe Nutzerakzeptanz zu erzielen.

Beim Einsatz von Netzwerken mit Microsoft-Lösungen bieten sich verschiedene Cloud-Dienste an, die für den sicheren Betrieb von Windows und Cloud-Komponenten von Microsoft optimiert sind. Auf diese Tools gehen wir nachfolgend genauer ein.

Schritt 5: Laufender Betrieb

Mit der erfolgreichen Implementierung der Prozesse, Anwendungen und Tools schließt Cyber Security nicht ab. Der dynamische Cyber War erfordert ein permanentes Monitoring der Umgebung, die Risikobewertung von Sicherheitsvorfällen und die unmittelbare Reaktion bei Gefahrensituationen. Diese Aufgaben übernimmt ebenfalls das SOC. Ein SOC kann ein Unternehmen entweder selbst betreiben oder auf externe SOCs zurückgreifen.



MICROSOFT 365 DEFENDER FÜR DEN SCHUTZ VON UNTERNEHMENSDATEN

Setzen Unternehmen auf Dienste und Betriebssysteme von Microsoft und Cloud-Dienste wie **Microsoft 365** und **Azure Cloud**, ist es sinnvoll auf Sicherheitstools zu setzen, die für die Cloud-Plattform optimiert sind. Microsoft 365 setzt für die Authentifizierung der Nutzenden Azure Active Directory ein, sodass für den Schutz der Konten Microsoft 365 und Azure parallel geschützt werden sollten. Hier spielt auch der Schutz der lokalen Anmeldedaten eine Rolle.

Microsoft 365 Defender und Microsoft Defender for Cloud bieten ein Bundle von verschiedenen Sicherheitsdiensten für die Nutzung von Azure und Microsoft 365. Bestandteil davon sind regelmäßige Berichte, die dabei helfen Schwachstellen zu identifizieren. Auf Basis dieser Vorhersagen ist es möglich, passgenaue Gegenmaßnahmen abzuleiten.

Im Fokus von Microsoft 365 Defender steht der Schutz von PCs, Nutzenden, Office-Anwendungen und deren Apps. Microsoft Defender for Cloud ist wiederum für den Schutz der Cloud, Server und sonstiger Infrastrukturen verantwortlich. Datenbanken lassen sich damit genauso schützen wie Workload-Server und Container. In Kombination schützen die beiden Systeme komplette IT-Infrastrukturen zuverlässig und intelligent. Um die Tools und Dienste optimal zu nutzen, sind individuelle Einstellungen und hohes Fachwissen notwendig.

Microsoft Defender for Endpoint

Mit Microsoft Defender for Endpoint bohrt Microsoft den vorhandenen Schutz in Windows 10 und Windows 11 deutlich auf und bindet die Systeme zentral an einen Cloud-Dienst an.

Unternehmen können zusammen mit externen IT-Spezialist:innen Richtlinien und Regeln definieren, mit denen Microsoft Defender Arbeitsstationen und unternehmenskritische Inhalte zuverlässig schützt. Der Microsoft Defender for Endpoint agiert als EDR-Tool (Endpoint Detection and Response) betriebsnah direkt auf den Geräten und betrachtet somit genauestens alle Prozesse, die auf einem Rechner ablaufen. Gleichzeitig ermöglicht das Tool den Mitarbeitenden im SOC direkt auf ein betroffenes Gerät zuzugreifen, diese zu isolieren oder schädliche Dokumente zu löschen. Kaum eine andere Technologie kann eine solch breite Angriffsfläche der bekannten Bedrohungslage abdecken und durch schnelle Handlungsmöglichkeiten die Ausfallzeiten Ihrer Mitarbeitenden bei aktiven Bedrohungen minimal halten. Interessant ist an dieser Stelle, dass Microsoft Defender for Endpoint auch macOS, Android, iOS und Linux vor Angriffen schützen kann.

Microsoft Defender for Office 365

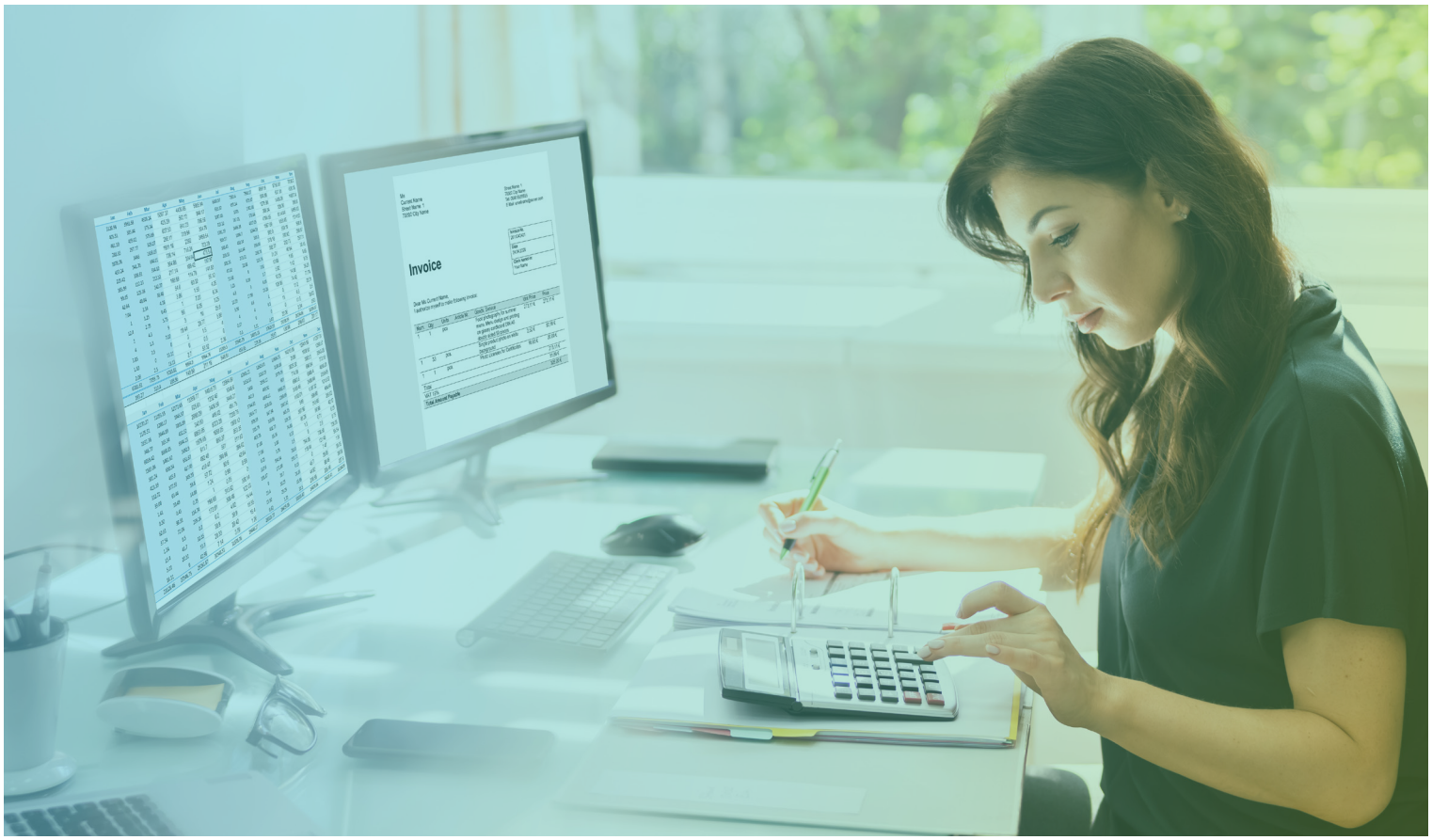
Ergänzend zum Schutz der Arbeitsstationen und Server mit Microsoft Defender for Endpoint, bietet Defender for Office 365 speziellen Schutz für E-Mails in Microsoft 365, Exchange Online und für Microsoft Office-Dokumente und -Programme. Auch hier nutzt Defender for Office 365 die bereits vorhandenen Funktionen wie zum Beispiel Exchange Online Protection und bindet diese in das System ein. Durch Sandboxing erhöht Microsoft Defender for Office 365 die E-Mail-Sicherheit mit den Funktionen Safe Link und Safe Attachments um ein Vielfaches – Anhänge und Links werden vor dem Öffnen in einer sicheren Umgebung von Microsoft (der Sandbox) ausgeführt und auf Schadprogramme untersucht. Das minimiert das Risiko für die Unternehmensdaten noch einmal deutlich, unabhängig vom Zugriffsort.

Der Elektrogroßhändler Möhle war im Februar 2020 drei Wochen lahmgelegt. Ein Mitarbeiter im Unternehmen hat eine E-Mail mit einem Virus geöffnet. Das ermöglichte den Angreifenden einen Fernzugriff. Diese haben den Zugriff dazu genutzt, alle PCs im Unternehmen lahmzulegen. Bei diesem Angriff wurde auch das Backup-System beschädigt, sodass die verlorenen Daten nicht mehr wiederherstellbar waren. Das Unternehmen hat das Lösegeld in Höhe von 120.000 Euro bezahlt, da die Existenz der Firma unmittelbar bedroht war. Solche Angriffe zu verhindern ist die Aufgabe von Microsoft Defender for Office 365 und Microsoft Defender for Endpoint.

Defender for Identity und Azure AD Identity Protection

Eine weitere Säule für mehr Sicherheit ist der Schutz der Konten von Anwendenden. Hier sind die beiden Dienste Defender for Identity und Azure AD Identity Protection das ideale Werkzeug. Microsoft Defender for Identity ist eine cloudbasierte Sicherheitslösung, die das lokale Active Directory auf gefährliches Anmeldeverhalten überwacht. Das Programm identifiziert und bekämpft komplexe Bedrohungen. Gefährdete Identitäten und schädliche Insideraktionen werden frühzeitig erkannt.

Der Werkzeughersteller Einhell aus Landau wurde 2019 Opfer eines Hackerangriffes. Dabei haben die Angreifenden große Datenmengen gestohlen. Die Cyberkriminellen drohten damit, die Daten zu veröffentlichen, wenn das Unternehmen kein Lösegeld bezahlt. Die Hacker:innen haben dazu eine E-Mail mit einem Virus an Mitarbeitende verschickt, um an Anmeldedaten der Nutzenden zu kommen. Ohne zuverlässigen Schutz durch Systeme wie Defender for Identity und Azure AD Identity Protection können Angreifende erbeutete Anmeldedaten leicht nutzen.



MANAGED MICROSOFT SECURITY SERVICES

Lösungen wie Microsoft 365 Defender und Microsoft Defender for Cloud bieten für sich allein gesehen nur grundlegenden Schutz. Die Anwendungen und Funktionen müssen regelmäßig aktualisiert und Berichte analysiert werden, andernfalls bieten die Tools nur eingeschränkte Schutzfunktionen. Darüber hinaus spielt die Korrelation der Informationen aus der gesamten Sicherheitsumgebung und insbesondere die zuverlässige Erkennung, Analyse sowie souveräne Response auf mögliche Bedrohungen eine entscheidende Rolle. Der Betrieb eines SOCs ist also unverzichtbar für eine umfassende und zuverlässige Cyber Security.

Oftmals verfügen Unternehmen (auch Unternehmen mit internem SOC) über Wissenslücken darüber, welche Anwendungen und Konfigurationen zielführend für die eigene Cyber Security sind. In diesem Fall – aber auch, wenn aus zeitlichen oder fachlichen Gründen kein internes SOC vorhanden ist – können Leistungen von externen Partnern sinnvoll sein, um nachhaltig in Advanced Security zu investieren.

Bei Arvato Systems bieten wir ein umfassendes und maßgeschneidertes Cyber Care Angebot für zuverlässige Advanced Cyber Security. Wir setzen bei einer individuellen Bedarfsanalyse an und bauen darauf eine professionelle und zielgerichtete Beratung mit Handlungsempfehlungen für die Sicherheitsstrategie auf. Auf Wunsch übernehmen wir auch die Implementierung und die Konfiguration der gewünschten Tools und sichern mit einem eigenen SOC schließlich auch den Betrieb der Advanced Security Leistungen ab. Die Leistungen der Managed Microsoft Security Services stellen wir unseren Kund:innen einzeln oder als Komplettpaket zur Verfügung, ganz nach individuellem Bedarf und Interesse. Die Managed Microsoft Security Services umfassen die gesamte Microsoft Referenzarchitektur einschließlich des Sensorbetriebs, einer Korrelationsebene mit Azure Sentinel als Managed Security Information and Event Management (SIEM) sowie den Managed Detection- und Response-Services.

Die fortlaufende Überwachung der Bedrohungslage und des Secure Score sorgen dafür, dass der Schutz immer ein Höchstmaß an Sicherheit bietet. Die aus verschiedenen Quellen gesammelten Daten werden regelmäßig korreliert, analysiert und die relevanten Regeln optimiert. Das ermöglicht eine gezielte und automatisierte Bekämpfung neuer Gefahren. Sobald das System einen Angriff erkennt, schreitet das SOC ein. Dabei erkennen die Fachkräfte auch hier Fehlalarme (False Positives). Echte Angriffe werden auf Basis vorher festgelegter und abgestimmter Maßnahmen bekämpft und abgewehrt.

SOC-Leistungen im Überblick

- Prevention (vorbeugende Maßnahmen)
- Detection (Monitoring des Systems)
- Response (Reaktion auf Sicherheitsvorfälle)

Mit den Managed Microsoft Security Services sind die Tools von Microsoft 365 Defender und Microsoft Defender for Cloud nicht mehr nur Bestandteil der IT-Umgebung. Die Tools werden zum aktiven Schutz für eine rundum gewährleistete Sicherheit durch künstliche Intelligenz optimiert und von zertifizierten IT-Spezialist:innen verwaltet. Unternehmen profitieren von einer neuen Dimension für Cyber Security. Dabei lässt sich das bereits vorhandene Fachwissen nutzen, ausbauen und als weitere Säule in das Sicherheitssystem einbinden, um auch zukünftigen Herausforderungen entgegenzustehen.

FAZIT

Die Gefahren für organisationsweite IT-Infrastrukturen sind real. Unternehmen müssen reagieren und den Schutz der Anwendenden auch im Home Office verbessern und optimieren. Dabei kommen idealerweise Standardtools von Microsoft zum Einsatz, die sich optimal in Microsoft-Umgebungen einbinden lassen und durch Best Practices ein Höchstmaß an Schutz bieten. Expert:innen können diese Dienste optimal in Unternehmen integrieren, überwachen und damit aktiv für den Schutz von Digital Workplaces und Workloads sorgen.

Start

Kontakt

Sie haben Fragen zu Advanced Security oder zum Whitepaper? Melden Sie sich gerne bei uns!

Timo Schlüter
Experte für Cyber Security
Telefon: +49 5241 80-40312
E-Mail: cybercare@arvato-systems.de

Impressum

Arvato Systems
Reinhard-Mohn-Straße 18
33333 Gütersloh

www.arvato-systems.de

www.twitter.com/arvatosystemsDE

www.youtube.com/user/arvatosys

Arvato Systems GmbH, Reinhard-Mohn-Straße 18, D-33333 Gütersloh
info@arvato-systems.de | arvato-systems.de