Petri IT Knowledgebase
Resource A BWW Media Group
Brand

PETRI
WE GET IT

Petri Whitepaper 10.
November 2022

Grundlegende Vorbereitung zur Cybersicherheit von KMUs

Gesponsert von Devolutions

Übersicht

Cybersicherheit ist eines der wichtigsten Anliegen der meisten IT-Unternehmen und die Umsetzung einer wirksamen Strategie zur Cybersicherheit war noch nie so schwierig wie heute.

Die heutigen Bedrohungen für die Cybersicherheit sind häufiger und ausgefeilter als je zuvor.

Die digitale Transformation und Ransomware-as-a-Service bringen neue Herausforderungen für die IT-Sicherheit.

Für die Zunahme von Cyberangriffen gibt es mehrere Gründe. Erstens befinden sich seit einigen Jahren die meisten kleinen und großen Unternehmen, Organisationen und sogar Regierungen inmitten einer digitalen Transformation, die es erforderlich macht, dass sie ihre Computersysteme aktualisieren und neue Technologien einführen. Dies hat dazu geführt, dass neue Technologien und Geräte eingeführt wurden, die nicht immer in das traditionelle Sicherheitsmodell passen.

Zweitens hat das Aufkommen von Ransomware-as-a-Service (RaaS) den Anstieg von Ransomware beschleunigt. Ebenso wie die Technologie für Unternehmen hat sich auch die der Cyber-Kriminellen weiterentwickelt. Die heutigen Cyber-Kriminellen sind gut ausgebildet und verfügen über eine große Auswahl leicht zugänglicher Hacking-Tools.

Die Anbieter von Ransomware-as-a-Service (RaaS) machen es auch Cyber-Kriminellen möglich, Ransomware-Angriffe zu starten, die selbst nicht über die notwendigen technischen Fähigkeiten verfügen, die zur Erstellung und zum Einsatz von Ransomware nötig sind.

Darüber hinaus hat die Pandemie zu einer raschen und massiven Zunahme von mobilen Mitarbeitern geführt. Dies hat die Angriffsfläche der Unternehmen erheblich vergrößert und eine Mischung aus schlecht gesicherten persönlichen Endgeräten erzeugt. Es ist klar, dass Unternehmen in absehbarer Zeit mit diesen Bedingungen zurechtkommen müssen.

Es ist wichtig, zu beachten, dass Cyber-Kriminelle ihre Angriffe nicht auf große Unternehmen beschränken. Zunehmend haben sie KMUs im Visier und attackieren andere verwundbare Einrichtungen wie Schulen, Krankenhäuser, Fertigungsbetriebe und sogar Infrastruktur-Dienstleister wie Gasleitungen und Elektrizitätswerke. Laut einer Studie von IBM und der Ponemon Group research by IBM and the Ponemon Group sind die Kosten einer Datenschutzverletzung für Unternehmen aller Größenordnungen auf durchschnittlich 4,24 Mio. USD pro Vorfall gestiegen - der höchste jemals ermittelte Betrag. Allein für KMUs kann der finanzielle Schaden zwischen 120.000 USD und 1,24 Mio. USD pro Vorfall liegen.

Es ist klar, dass IT-Sicherheit und Cybersicherheit ein teures und wachsendes Problem darstellen. Daher ist es auch wichtig, zu verstehen, dass Sicherheit nicht nur ein technisches Problem ist. Heutzutage ist sie von grundlegender Bedeutung, um das Überleben eines Unternehmens zu gewährleisten. Werfen wir einen genaueren Blick auf einige der wichtigsten Bereiche, auf die sich KMUs konzentrieren müssen.

Bewertung von Bedrohungen für die IT-Sicherheit und Cybersicherheit

Die Sicherheitsbedrohungen und deren Schweregrad nehmen zu. In der Umfrage von Devolutions zum Stand der IT-Sicherheit in KMUs im Jahr 2022-2023 wurden Führungskräfte und Entscheidungsträger in

KMUs weltweit darum gebeten, ihren Gesamteindruck zur IT-Sicherheit zu beschreiben. Sie wurden gefragt: **„*Wie besorgt sind Sie im Vergleich zum letzten Jahr über Bedrohungen der Cybersicherheit für Ihr Unternehmen?*”** Zwei Drittel (67 %) antworteten: ***„Wir sind besorgter als letztes Jahr“***,
28 % antworteten sie seien ***„genauso besorgt”*** und 5 % waren ***„weniger besorgt.”***

Die Tatsache, dass 67 % der Unternehmen besorgter sind, macht deutlich, dass sich die meisten auf vermehrte Cyber-Angriffe vorbereiten. Allerdings zeigte sich fast ein Drittel ebenso besorgt und gab an, dass sie möglicherweise keine angemessenen Vorkehrungen für eine künftige Eskalation von Angriffen treffen werden. Die 5 % weniger Besorgten lassen sich möglicherweise darauf zurückführen, dass viele Unternehmen ihre mobilen Mitarbeiter in die Büros zurückrufen und so die Sicherheitskontrollen verschärfen können.

Es überrascht nicht, dass auf die Frage nach den Arten von Bedrohungen der Cybersicherheit, die ihnen die größten Sorgen bereiten, die meisten Unternehmen (81 %) sich von Ransomware bedroht fühlen, gefolgt von:

- Phishing (69 %)
- Malware (38 %)
- und internen Bedrohungen (21 %)

In Anbetracht der kontinuierlichen Zunahme von Ransomware ist es klar, dass dies ein Bereich ist, in dem sich KMUs auf verstärkte Angriffe vorbereiten müssen.

Sicherung der Software von Drittanbietern und der Lieferkette

Ein wichtiger Bereich, der bisher nicht genannt wurde, waren Angriffe auf Software von Drittanbietern oder auf die Lieferkette. Der jüngste Angriff auf die Lieferkette von SolarWinds/Solarigate SolarWinds/Solarigate supply chain attack, von dem tausende von Unternehmen betroffen waren, zeigt deutlich, wie wichtig es ist, die Software von Drittanbietern zu überprüfen, um sicherzustellen, dass sie den höchsten Sicherheitsansprüchen gerecht wird.

13 % der KMUs ergreifen keine Maßnahmen zur Verhinderung von Cyber-Angriffen

Die Bewertung von Bedrohungen der Cybersicherheit ist ein wichtiger erster Schritt, um die Gefahren der verschiedenen Angriffe auf die Cybersicherheit zu verstehen und angemessen zu reagieren. Während sich die meisten Unternehmen auf die Zunahme von Ransomware, Phishing und Malware vorbereiten, hat die Umfrage auch ergeben, dass 13 % der KMUs überhaupt keine Maßnahmen ergreifen, um diese Arten von Angriffen zu verhindern.

KMUs mögen nur über begrenzte Ressourcen verfügen, aber dennoch ist klar, dass die Cybersicherheit ein Bereich ist, der nicht einfach ignoriert werden kann, wenn man sich nicht einer Gefahr aussetzen will.

Implementierung von Privilegierter Zugriffsverwaltung

Privilegierte Zugriffsverwaltung (PAM) bezieht sich auf die Verwaltung von administrativen Konten und Konten mit erhöhten Sicherheitsrechten, die Wartungsarbeiten, Systemänderungen und andere Arten von privilegierten Operationen zulassen. Diese privilegierten Konten sind häufig Ziel von Cyber-Angriffen, da sie Zugang zu hochsensiblen, vertraulichen und firmeneigenen Informationen gewähren.

Daher haben der Schutz und die Verwaltung dieser privilegierten Konten hohe Priorität. PAM-Lösungen gehen dieses Problem an. PAM reduziert die Sicherheitsrisiken durch den Schutz der Konten mit erhöhten Privilegien, senkt gleichzeitig die Betriebskosten und erhöht die Transparenz bei der Nutzung dieser Art von Konten.

Bei der ***Umfrage von Devolutions zum Stand der IT-Sicherheit in KMUs im Jahr 2022-2023*** gaben auf die Frage ***„Wie verwalten Sie hauptsächlich den Zugang zu privilegierten Konten in Ihrem Unternehmen?"*** nur 12 % der Unternehmen an, dass sie eine vollständig implementierte PAM-Lösung im Einsatz haben. Weitere 9 % gaben an, dass sie eine teilweise implementierte PAM-Lösung haben, bei der sie einige der Funktionen nutzen, aber nicht alle.

Nachfolgend wurde nach den Gründen gefragt, warum einige KMUs keine PAM-Lösungen einsetzen. Die Umfrage ergab, dass 28 % der Unternehmen nicht über das nötige Budget verfügten. Weitere 12 % waren der Meinung, dass PAM-Lösungen zu komplex seien, um sie zu implementieren und zu verwalten. Diese Sichtweisen sind verständlich. Allerdings sind sie veraltet und nicht mehr zutreffend.

PAM-Lösungen sind jetzt erschwinglich und einfach zu implementieren

Ursprünglich waren PAM-Lösungen preislich auf große Unternehmen zugeschnitten und für KMUs unerschwinglich. Außerdem konnten sich KMUs kein Team von internen Spezialisten für Cybersicherheit leisten, um diese älteren Lösungen zu konfigurieren und zu nutzen. Dies hat sich jedoch im Laufe der Jahre geändert. Inzwischen gibt es mehrere benutzerfreundliche PAM-Lösungen, die für KMUs erschwinglich sind.

Die Implementierung einer PAM-Lösung ist ein wichtiger Schritt, um KMUs auf eine stärkere Cybersicherheit vorzubereiten. Die Umfrage hat auch ergeben, dass die drei wichtigsten Funktionen, die KMUs von einer PAM-Lösung erwarten, folgende sind:

1. automatisch auslaufender privilegierter Zugriff
2. integrierte Multi-Faktor-Authentifizierung (MFA)
3. Passwortrotation und -zurücksetzung

Heutige PAM-Lösungen bieten diese Art von Automatisierung und machen sie daher effizient und gut geeignet für die Bedürfnisse
von KMUs.

Förderung des Sicherheitsbewusstseins der Endnutzer

Leider können die meisten Maßnahmen zur Cybersicherheit von Ihren Endnutzern umgangen werden. Sie sind das schwächste Glied in der IT-Sicherheitskette. Und es gibt eine Vielzahl von Möglichkeiten, wie Nutzer selbst die besten Sicherheitspläne sabotieren können.

Einige der größten Probleme sind schwache Passwörter (wie „Passwort"), die Wiederverwendung von Passwörtern auf mehreren Websites, die Weitergabe von Passwörtern, das Aufschreiben von Passwörtern, das Anklicken von Phishing-Links, die Malware herunterladen und der Zugriff auf Unternehmensressourcen über unsichere öffentliche WLAN-Verbindungen.

Die Vielfalt der Möglichkeiten, wie Endnutzer Sicherheitslücken verursachen können, ist nahezu endlos. Laut dem Verizon Data Breach Investigations Report (DBIR) for 2022 waren im vergangenen Jahr bei 82 % der Sicherheitsverletzungen Mitarbeiter der betroffenen Unternehmen involviert.

Der beste Weg, um Sicherheitsprobleme von Endnutzern anzugehen, ist eine Schulung des Sicherheitsbewusstseins. Bei der ***Umfrage von Devolutions zum Stand der IT-Sicherheit in KMUs im Jahr 2022-2023*** wurde die Frage gestellt ***„Wie bildet Ihr Unternehmen überwiegend die Endnutzer in IT-Sicherheit aus?"*** Etwa ein Drittel (30 %) verlässt sich ausschließlich auf Ressourcen wie Videos, Artikel und Webinare. Ein weiteres Drittel (31 %) nutzt Online-Schulungen. Eine viel kleinere Anzahl (16 %) nutzt Live-Schulungen und Workshops oder Simulationen (5 %). Und 12 % tun überhaupt nichts. Keine Schulung der Endnutzer kommt praktisch einer Einladung einer wie auch immer gearteten Sicherheitsgefährdung gleich.

Die überwiegende Mehrheit der KMUs (88 %) bietet irgendeine Form von Schulung für Nutzer an. Das ist gut. In Anbetracht der hohen Kosten, die ein Eindringen in die Cybersicherheit verursacht und der Erkenntnis, dass die meiste Gefahr von den Endnutzern ausgeht, unterstreichen diese Fakten die essenzielle Tatsache, dass dies einer der Bereiche ist, in dem erhöhte Investitionen zu einem verbesserten Schutz führen. Die Kosten für die Schulung der Nutzer sind belanglos im Vergleich zu den Kosten eines erfolgreichen Angriffs auf die Cybersicherheit, der ein KMU komplett vom Markt nehmen könnte.

Absicherung der Remote-Verbindungsverwaltung

In den letzten Jahren hat die Pandemie dazu geführt, dass der Einsatz von Tools für den Remote-Zugriff in Unternehmen aller Größenordnungen sprunghaft angestiegen ist. Dies hat zwar Mitarbeitern ermöglicht, von zu Hause aus auf Unternehmensressourcen und -anwendungen zuzugreifen, andererseits aber auch die Angriffsfläche der Unternehmen erheblich vergrößert.

Der Remote-Zugriff ermöglicht Mitarbeitern, sich mit lokalen Bürosystemen zu verbinden, um ihre Arbeit zu verrichten oder Administratoren, verschiedene Verwaltungsaufgaben aus der Ferne auszuführen. Erwartungsgemäß benötigen IT-Administratoren und Manager oft privilegierte Anmeldeinformationen. Schwache Passwörter, die leicht zu erraten sind, oder wiederverwendete Passwörter, die von anderen Websites abgegriffen werden können, können Hackern Tür und Tor öffnen. Sobald ein Cyber-Krimineller Zugang zu Ihrem Netzwerk erlangt hat, kann er von dort auf andere Systeme innerhalb Ihrer Netzwerke zugreifen.

Um den Umfang der derzeitigen Nutzung von Remote-Zugriffen ermessen zu können, wurden die KMUs in der Umfrage gefragt: ***„Wie sieht die derzeitige Situation beim Mitarbeitereinsatz in Ihrem Unternehmen aus?"*** Wie erwartet lässt die Mehrheit (75 %) hybride Arbeitsweisen zu, bei denen die Mitarbeiter ihre Zeit zwischen Büro- und Heimarbeitsplatz aufteilen. Nur 19 % lassen alle ihre Mitarbeiter Vollzeit im Büro arbeiten und geringe 6 % arbeiten vollständig mobil. Diese Ergebnisse zeigen, das mobiles Arbeiten und Technologien für den Remote-Zugriff nach wie vor weit verbreitet sind und dies wahrscheinlich auch noch einige Zeit bleiben werden, vielleicht sogar auf Dauer.

Nachfolgend wurde nach den Tools und Technologien gefragt, die die Unternehmen zur Absicherung und

Verwaltung des

Remote-Zugriffs verwenden. Die drei populärsten Lösungen waren:

- Virtual Private Network (VPN)
- Multi-Faktor-Authentifizierung
- Devolutions Remote Desktop Manager (RDM)

Die Pandemie hat zu einem erheblichen Anstieg des VPN-Einsatzes für mobile Mitarbeiter geführt. Und viele Unternehmen nutzen MFA als zusätzliche Sicherheitsebene, sodass mobil arbeitende Mitarbeiter ihre Identität nachweisen müssen, indem sie ihre Anmeldeinformationen zusammen mit einer anderen externen Information wie einem Code, der an ein Mobiltelefon gesendet wird, eingeben.

Devolutions RDM organisiert nicht nur Ihre Remote-Verbindungen, sondern verstärkt durch seine Möglichkeiten der Passwortverwaltung auch deren Sicherheit. Die Passwortverwaltung von RDM unterstützt Passwortrichtlinien, die die Länge und Komplexität von Passwörtern vorschreiben und die Wiederverwendung von Passwörtern einschränken. Zusätzliche Tools wie ein Passwortgenerator und ein Passwort-Analysator können es Nutzern erleichtern, sichere Passwörter zu erstellen und zu verwenden.

Mit RDM werden die Passwörter zentral an einem sicheren Ort gespeichert, sodass die Nutzer nicht länger ihre eigenen willkürlichen und unsicheren Methoden zur Speicherung von Passwörtern einsetzen müssen. Zudem kann RDM auch eine Übersicht und ein Protokoll aller Aktivitäten auf dem Remote-Desktop Ihrer Organisation liefern.

Planung des Managements der IT-Cybersicherheit

Ein umfassendes Management der IT-Cybersicherheit besteht aus Strategien, Richtlinien, Prozessen, Technologien und Tools, die den Schutz, die Integrität und die Verfügbarkeit von IT-Systemen gewährleisten. Angesichts der ständig zunehmenden Bedrohungen und des Zustroms neuer Technologien, die es zu schützen gilt, könnte man meinen, dass die Sicherheit einen beträchtlichen Teil des IT-Budgets eines KMU in Anspruch nehmen würde. Dies ist jedoch überraschenderweise nicht der Fall.

Auf die Frage, wie viel des IT-Budgets Ihres Unternehmens für die Sicherheit bereitgestellt wird, antwortete ein Drittel (32 %), dass es weniger als 5 % sind. Der Betrag, den ein Unternehmen für die Cybersicherheit ausgeben muss, ist zwar von Unternehmen zu Unternehmen sehr unterschiedlich, aber 5 % scheinen dem heutigen Bedrohungsniveau nicht mehr angemessen zu sein.

58 % gaben an, dass sie weniger als 20 % und nur 10 %, dass sie mehr als 20 % ihres Budgets für die Sicherheit aufwenden. 49 % meldeten einen Anstieg der Ausgaben für Sicherheit, aber 45 % gaben an, dass sie gleich geblieben seien. Das mag auf den ersten Blick unzureichend erscheinen. Die Unternehmen müssen jedoch auch das allgemeine Geschäftsumfeld berücksichtigen.

Die Pandemie hat bei vielen Unternehmen beispiellosen finanziellen Schaden zugefügt. Eine Studie der Federal Reserve (Zentralbank-System der USA) a study conducted by the Federal Reserve ergab, dass zwischen April 2020 und April 2021 schätzungsweise 200.000 KMUs in den USA als direkte Folge der Pandemie dauerhaft geschlossen wurden. Für viele KMUs war die Reduzierung der IT-Sicherheitsausgaben eher eine Notwendigkeit als ein Wunsch.

Zu den wichtigsten Sicherheitsprojekten, die die Unternehmen für die Zukunft in Betracht ziehen, gehören: PAM-Lösungen, 2FA (Zwei-Faktor-Authentifizierung, auch bekannt als MFA), Schulung der Endnutzer, Aktualisierung der VPN-Strategien, Implementierung einer automatischen Passwortrotation und Erweiterung der Passwortverwaltung. Alle diese häufig genannten

IT-Sicherheitsprojekte stehen im Zusammenhang mit der Identitäts- und Zugangsverwaltung, zwei zentralen Grundpfeiler für

effektive Cybersicherheit.

Vorbereitungen für den Schutz

Nirgendwo ist die Aussage „gute Planung vermeidet schlechte Leistung" zutreffender als im Bereich der Cybersicherheit. Unternehmen befinden sich heute an einem wichtigen Wendepunkt, da sich ihre digitalen Spuren ständig verändern und weiterentwickeln, wodurch viele ältere, etablierte Maßnahmen zur Cybersicherheit veralten; gleichzeitig nehmen die Bedrohungen zu und neue Bedrohungen entstehen.

Die Bedeutung der Cybersicherheit für KMUs wird weiter zunehmen, und sie müssen sich auf diese neuen Bedrohungen vorbereiten. Gleichzeitig müssen KMUs aber auch sicher sein, dass sie den größtmöglichen Nutzen aus ihren Investitionen für die Sicherheit ziehen.

Heutzutage erfordern die Vorbereitungen für Cybersicherheit eine Kombination von Faktoren, um aktuellen Bedrohungen wie Ransomware, Malware und Phishing zu begegnen. Die Planung der Vorbereitungen für Cybersicherheit erfordern, dass KMUs die Sicherheitstechnologien, die sie einsetzen, neu überdenken, damit sie den heutigen anspruchsvollen neuen Bedrohungen entgegentreten können.

Starke Passwörter und Passwortrichtlinien, wie sie von Devolutions RDM unterstützt werden, bieten ein wesentliches Maß an Schutz, indem sie schwache und wiederverwendete Passwörter eliminieren. Die Implementierung einer PAM-Lösung wie Devolutions Server hilft sicherzustellen, dass privilegierte Konten überwacht werden und dass die Nutzer über ein angemessenes Sicherheitsniveau verfügen, um ihre Arbeit effektiv erledigen zu können.

Es ist wichtig, das Sicherheitsbewusstsein der Endnutzer zu stärken, um sicherere Arbeitsweisen zu fördern. Darüber hinaus müssen Unternehmen heute sicherstellen, dass ihre Lieferketten geschützt sind und dass die Unternehmen, mit denen sie Geschäfte machen, über solide IT-Sicherheitsmaßnahmen und bewährte Verfahren verfügen.

Weitere Einblicke in den Stand der Cybersicherheit für KMUs finden Sie im Bericht zur ***Umfrage von Devolutions zum Stand der IT-Sicherheit in KMUs im Jahr 2022-2023.***

Zusätzliche Informationen

Weitere ausführliche Information über die Herausforderungen und Lösungen im Bereich der Cybersicherheit für KMUs finden Sie hier: Devolutions State of Cybersecurity in SMBs in the 2021 report.