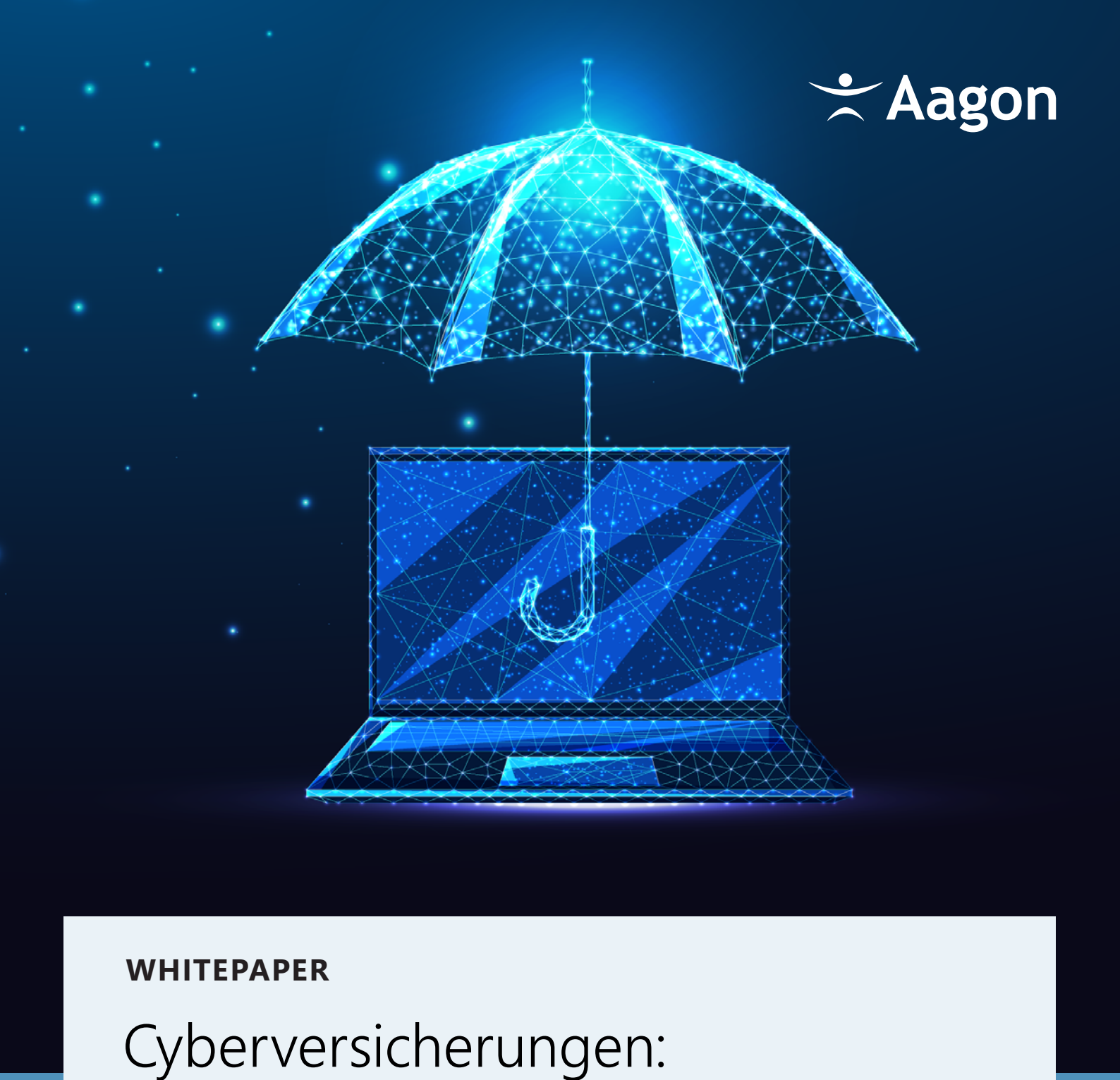


WHITEPAPER

Cyberversicherungen: Warum immer mehr Unternehmen darauf angewiesen sind

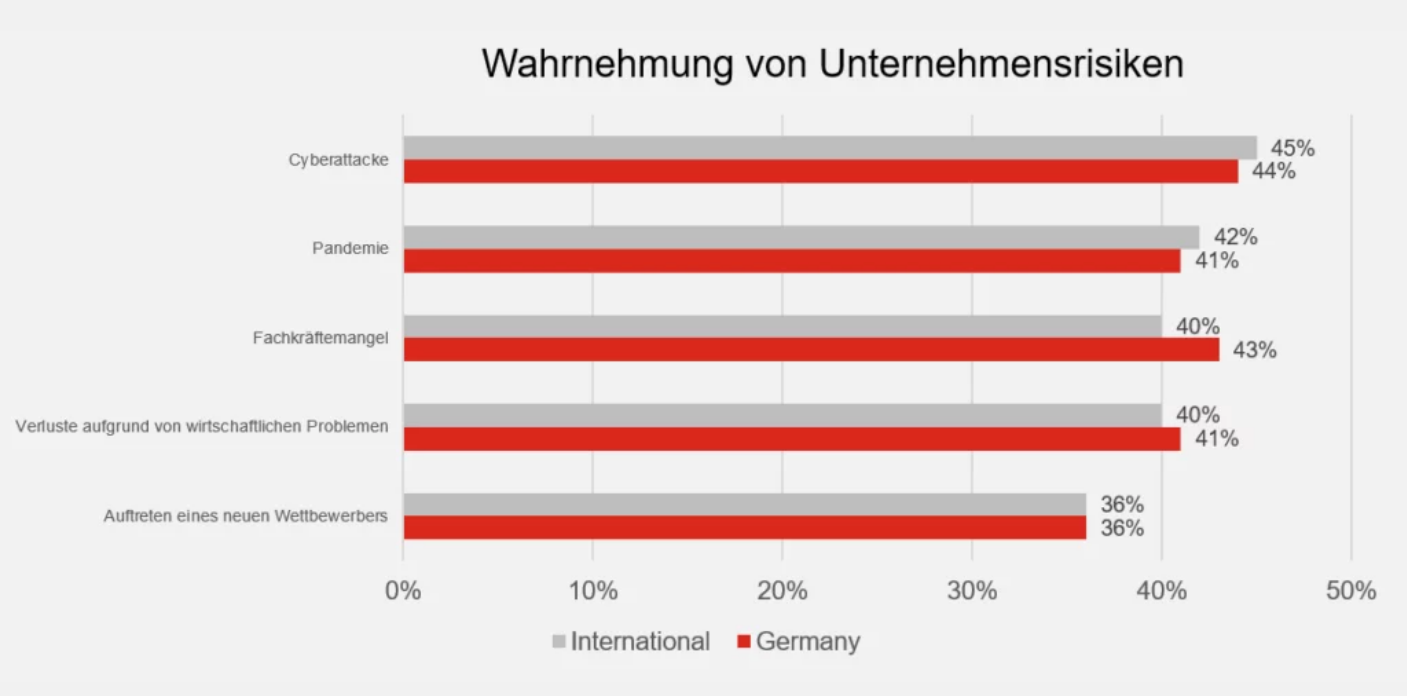
In Zeiten rasant zunehmender Bedrohungen durch Cyberkriminelle schützen sich immer mehr Unternehmen mit einer Cyberversicherung. Warum? Das erfahren Sie hier.

Januar 2024

www.aagon.com

Was ist eine Cyberversicherung und warum ist sie nötig?

Aktuelle Entwicklungen machen Cyberversicherung unabdingbar. Der IT-Branchenverband Bitkom berichtet in einer Studie aus 2022, dass **9 von 10 Unternehmen Opfer von Datendiebstahl, Spionage oder Sabotage werden und die Rolle der organisierten Kriminalität bei den Attacken stetig zunimmt. Der dadurch entstehende Schaden der deutschen Wirtschaft beläuft sich auf etwa 203 Milliarden Euro pro Jahr.** Auch der Hiscox Cyber Readiness Report 2022 zeigt deutlich: Cyberangriffe sind Risiko Nummer eins für Unternehmen und stellen somit eine enorme Bedrohung dar.



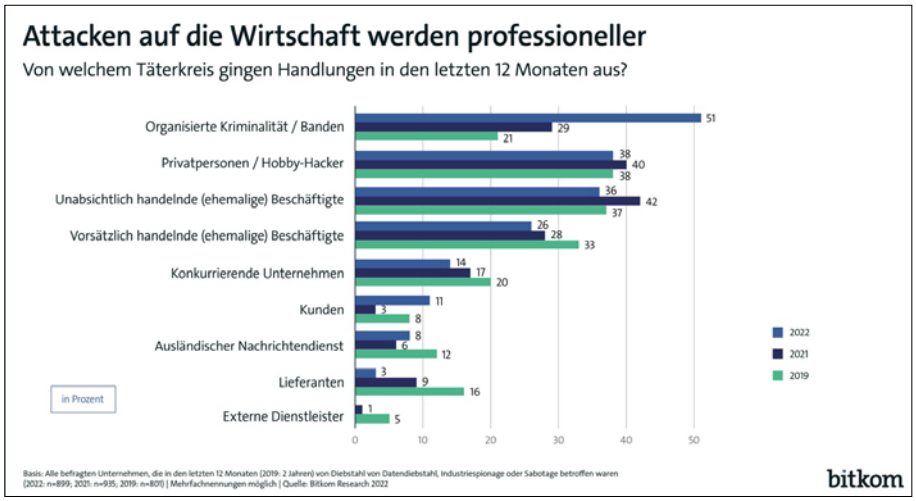
Quelle: https://www.hiscox.de/cyber-readiness-report-2022/

Definition

Eine Cyberversicherung ist eine spezielle Versicherung, die Unternehmen vor den finanziellen Folgen von Cyberangriffen schützt. Sie deckt also Kosten ab, die im Zusammenhang mit Sicherheitsverletzungen, Datenverlusten, Haftungsansprüchen und anderen Schäden durch Cyberkriminalität oder Datenschutzverletzungen entstanden sind.

Welchen Ursprung haben die Cyberangriffe?

Durch den technologischen Fortschritt finden Cyberkriminelle und die, die es werden wollen, im sogenannten Darknet nicht nur die Informationen und Werkzeuge, die sie benötigen. Sondern sogar Dienstleister, die solche Angriffe für sie ausführen. Außerdem stellen vom Firmennetzwerk entkoppelte mobile Devices wie der kaum gewartete Laptop im Homeoffice sowie Smartphones eine Gefahr dar. Die Verlockung wächst also – und damit auch der Kreis potenzieller Täter.



Quelle: https://www.hiscox.de/cyber-readiness-report-2022/

Wichtig ist außerdem, dass nicht nur solche Unternehmen angegriffen werden, die über sensible Daten wie Bankdaten oder Krankenakten verfügen. Sondern jeder Betrieb Ziel von Hackern wird. Denn auch der Raub von weniger sensiblen Daten bringt Rufschädigung und Schadensersatzansprüche mit sich.

Die wichtigsten Begrifflichkeiten: Was wird abgesichert?

Eine Cyberversicherung kann

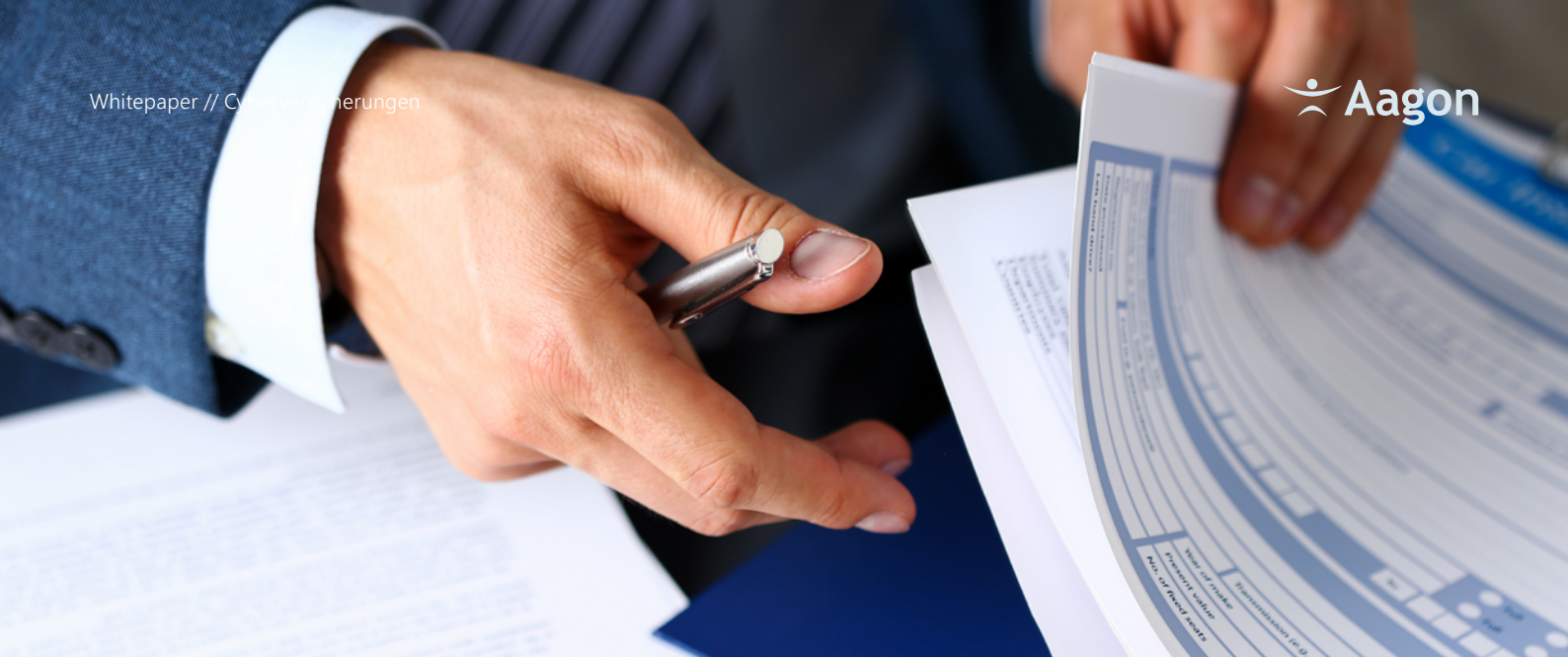
- **Kosten** für die Untersuchung von Sicherheitsverletzungen, das Benachrichtigen von Betroffenen, die Einrichtung von Callcentern für Kundenunterstützung sowie für forensische Analysen und Datenwiederherstellung abdecken

- **Haftungsansprüche** abdecken, die sich aus Verletzungen der Privatsphäre, Verlust oder Diebstahl von Kunden- oder Geschäftsdaten oder anderen Datenschutzverletzungen ergeben

- **Unterstützung durch Experten** bieten: bei der Schadensbegrenzung, der Wiederherstellung der Systeme und der Stärkung der Sicherheitsmaßnahmen

- finanzielle **Verluste** infolge einer Betriebsunterbrechung aufgrund von Cyberangriffen oder Datenverletzungen abdecken (Umsatzeinbußen während der durch den Angriff unproduktiven Zeit)

- Kosten für **rechtliche Verteidigung** und rechtliche Streitigkeiten abdecken, die aus Datenschutzverletzungen oder anderen Cyber-Vorfällen resultieren können sowie Strafen oder Geldbußen abdecken, die aufgrund von Verstößen gegen Datenschutzbestimmungen verhängt werden



Welche Kosten- und Berechnungsgrundlagen nutzen Cyberversicherungen?

1. Bereits implementierte **Cybersecurity-Maßnahmen** wie Firewalls, Verschlüsselung, regelmäßige Sicherheitsüberprüfungen oder Mitarbeiter-Schulungen wirken sich positiv auf die Versicherungsprämien aus und sind häufig Voraussetzung dafür, dass ein Vertrag überhaupt abgeschlossen werden kann.

2. **Unternehmensgröße und Branche**: Parameter sind neben Qualität sowie Quantität auch die Sensibilität der Daten je nach Compliance-Anforderungen, die in manchen Bereichen wie Gesundheitswesen und Finanzsektor deutlich höher sind.

3. **Umsatz und Jahresgewinn** beeinflussen die Berechnung dahingehend, dass potenzielle Einbußen abhängig von den generierten Einnahmen deutlich mehr Kosten verursachen würden.

4. Die Höhe der festgelegten **Deckungssumme und Selbstbeteiligung** beeinflussen die Prämien.

5. Frühere **Sicherheitsverletzungen und Datenverluste** können zu angepassten Versicherungsprämien führen.

Welche Probleme treten bei Cyberversicherungen auf?

1. **Ausschlüsse**: Einige Arten von Angriffen oder Schäden können nicht abgedeckt sein. Auch kann es Obergrenzen für bestimmte Arten von Verlusten oder Kosten geben.

2. **Komplexität**: Um eine passende Preiskalkulation zu generieren, sind die Sicherheitsmaßnahmen, IT-Infrastruktur sowie Branche des Unternehmens zu bewerten. Oftmals sind Berechnungen und Ergebnisse schwer nachzuvollziehen.

3. **Standards**: Aufgrund der relativ jungen Branche gibt es keine flächendeckenden Maßstäbe für Bedingungen und Policen. Somit ist eine sorgfältige Prüfung aller Angaben nötig.

4. **Schadensbewertung**: Für Versicherungen ist es schwierig, die finanziellen Auswirkungen eines Angriffs – wie den Verlust bestimmter Daten oder einer Rufschädigung – zu ermessen.

5. **Dynamik**: **Cyberbedrohungen verändern sich stetig**. Somit sind viele neu entstehende Angriffstechniken und Schwachstellen nicht im Versicherungsschutz enthalten, weil sie zum Zeitpunkt des Abschlusses noch nicht bekannt waren.

Welche Voraussetzungen müssen Unternehmen erfüllen, um eine Cyberversicherung abschließen zu können?

Obwohl es aus oben genannten Gründen für jedes Unternehmen ratsam ist, eine Cyberversicherung abzuschließen, weisen Versicherer viele Anfragen ab. Damit das nicht passiert, müssen folgende Anforderungen erfüllt sein.

1. Vorhandene Sicherheitsmaßnahmen

Unternehmen müssen nachweisen, dass es über angemessene Sicherheitsvorkehrungen verfügt. Dazu gehören Firewalls, Antivirus-Software, regelmäßige Software-Updates, sichere Zugriffskontrollen und andere Schutzmaßnahmen.

2. Gelebte Sicherheitsrichtlinien

Auch ist es essenziell, dass Mitarbeiter bestimmte Sicherheitsrichtlinien für die Nutzung von IT-Systemen und den Umgang mit Passwörtern einhalten. Dazu müssen Unternehmen Schulungen zur Cybersicherheit nachweisen.

3. Bestimmte Größe

Erfüllen Unternehmen die von der Versicherung vorgegebenen Parameter bezüglich Umsatz, Anzahl der Mitarbeiter oder bestimmter finanzieller Kennzahlen nicht, können sie keine Cyberversicherung abschließen.

4. Minimales Risiko

Auch Risikobewertungen der bestehenden Sicherheitsmaßnahmen sind bei einigen Cyberversicherungen erforderlich. Dazu gehören Prüfberichte über die Netzwerksicherheit, Penetrationstests oder Sicherheitsaudits. Erstellt werden diese von spezialisierten Dienstleistern, die sowohl vor als auch nach Einführung der Lösung prüfen.

5. Durchdachter Plan

In einem Incident-Response-Plan definieren Unternehmen den Umgang mit Sicherheitsvorfällen und Datenverletzungen. Dies umfasst die Meldung von Vorfällen, deren Untersuchung und Behebung ebenso wie die Benachrichtigung betroffener Parteien.

Wie kann eine Client Management Lösung dabei unterstützen, eine Cyberversicherung zu bekommen – und das zu bestmöglichen Konditionen?

Die Aagon Client Management Platform (ACMP) bietet genau das, was Versicherungen fordern: nicht einzelne, getrennt voneinander wirkende Maßnahmen, sondern ein **komplexes Konzept**. Dieses generiert eine umfassende **Sicherheit für Unternehmen** – und schafft somit die bestmögliche Basis für einen tragenden Versicherungsschutz.

Was ist ACMP?

ACMP ist eine auf individuelle Kundenbedürfnisse ausgerichtete **modulare Lösung für die Automatisierung der IT**, die zentral verwaltet wird. Das Ziel: Für maximale Sicherheit, hohen Bedienungskomfort und übergreifende Transparenz in allen Prozessen zu sorgen – und zwar **proaktiv sowie reaktionsschnell.**

Welche ACMP Module unterstützen die Cybersicherheit?

Um die Cybersicherheit zu gewährleisten, eignen sich die folgenden Module:

1. ACMP Defender Management

Das ACMP Defender Management bietet die **Grundlage für eine Verwaltung des in Microsoft enthaltenen Antivirusschutzes**. Das Modul zeigt den Defender-Status im Modul Dashboard. Hier erkennen IT-Administratoren direkt, welche Clients managebar sind. Außerdem sehen sie, von welchen die meisten sowie die letzten Alarme ausgegangen sind und wie oft welche Signatur verteilt ist. Durch diesen Überblick in nahezu Echtzeit sind neuste Bedrohungen stets sichtbar. Außerdem sind darüber diverse Abfragen zu Quarantänedateien möglich. In der zentralen Quarantäneverwaltung können Nutzer die als schädlich identifizierten Dateien löschen oder auch wiederherstellen.

2. ACMP Schwachstellenmanagement

Schwachstellen in Client-Umgebungen entstehen durch veraltete Programme, Sicherheitslücken und fehlerhafte Konfigurationen. Damit ein IT-Administrator **kritische Schwachstellen frühestmöglich und zielgerichtet ausbessern** kann, unterstützt dieses Modul. Dabei führt es umfassende Sicherheitsscans aller Windows-Clients durch und gibt CVSS- und CVE-zertifizierte Handlungsempfehlungen.

3. ACMP BitLocker Management

Das ACMP BitLocker Management ergänzt den Microsoft BitLocker um praktische Funktionen. Dieser verschlüsselt sowohl Betriebssystem- als auch Festplattenlaufwerke, um **unternehmensinterne Daten im Falle eines Diebstahls zu schützen**. Das ACMP BitLocker Management ermöglicht den IT-Administratoren eine zentrale und nativ konfigurier- und steuerbare Verwaltung. Außerdem ist das Modul durch das Basis Modul ACMP Core mit einer umfassenden Reportfunktion ausgestattet.

Welche Synergieeffekte ergeben sich mit weiteren Modulen?

Auch Module aus dem Bereich Managen und Verteilen unterstützen die Sicherheit der IT von Unternehmen. Dazu gehören:

1. ACMP Managed Software

IT-Administratoren verbringen viel Zeit damit, **Updates, Patches sowie Releases zu verwalten und Software zu paketieren**. ACMP Managed Software übernimmt diese Aufgabe durch vorpaketierte Software-Bundles, sodass sicherheitsrelevante Updates vor ihrer Bereitstellung bereits geprüft sind. Zudem ist es möglich, individuelle Test- und Freigabeprozesse zu definieren und dadurch die Kompatibilität der unternehmensinternen Systemlandschaft zu prüfen. So ist ein automatisches Update- und Patch Management von vielen Standardprogrammen sichergestellt. Nicht zuletzt sorgt die integrierte Clean-up-Automation dafür, dass alte Softwarepakete gelöscht werden.

2. ACMP CAWUM

CAWUM bedeutet Complete Aagon Windows Update Management und **löst die Microsoft Windows Server Update Services (WSUS) ab**. Unternehmen profitieren von automatisierten sowie individualisierten Updates, die Zeit und Bandbreite sparen. Dank CAWUM reagieren IT-Administratoren auf Patches oder Bedrohungen ganz nach Bedarf – tagesaktuell, vollautomatisch oder individuell gesteuert. Die ebenfalls integrierte automatische Aufräumfunktion schafft einen übersichtlichen Stand bei Updates und gibt unnötig belegten Speicherplatz frei. Individuelle Verteilprozesse geben überdies Updates entweder für alle gleichzeitig frei oder lassen sie verschiedene Testringe durchlaufen – je nach Update vom Administrator anpassbar, was im Gegensatz zum WSUS eine deutlich granularere Steuerung ermöglicht.

3. ACMP Desktop Automation

Die intuitiv bedienbare Desktop Automation ist das technologische Herz von ACMP. Mithilfe von mitgelieferten sowie selbst erstellten Client Commands sorgt sie für die **Automatisierung der administrativen Aufgaben** – selbst komplizierter Prozesse – auf Server- und Clientsystemen. Es wird ein umfassender Baukasten mit bereits vorbereiteten Bausteinen mitgeliefert. Hierüber können z.B. eigene PowerShell Skripte ausgeführt werden, Software individuell paketiert und verteilt werden. Client Commands können den Nutzern über diverse Möglichkeiten zur Verfügung gestellt werden, z.B. als Self Service durch den ACMP Kiosk. Paketierte Software kann so bei Bedarf selbst und nutzerfreundlich nach IT-Vorgaben installiert werden. Auch automatische Reaktionen auf Ereignisse bspw. aus dem ACMP Defender Management sind möglich, um weitere Maßnahmen einzuleiten.

Checkliste für die optimale Cyberversicherung

Die folgende Checkliste gibt nochmals einen zusammenfassenden Überblick über die wichtigsten Schritte innerhalb des Prozesses zum Abschluss einer Cyberversicherung.

Schritt	Notiz	Erledigt
1. Risikobewertung: Spezifische Risiken des Unternehmens ausmachen		
2. Risikoanalyse: Deckungsbedarf unternehmens-spezifisch festlegen		
3. Cybersecuritymaßnahmen: Maßnahmen treffen, um höchstmögliche Absicherung zu gewährleisten *Tipp: Komplexes Konzept von aufeinander aufbauenden Maß-nahmen wie ACMP wählen*		
4. Versicherungsvergleich: Angebote einholen und von unabhängigem Experten bewerten lassen		
5. Kosten-Nutzen-Analyse: Versicherungsbeitrag im Verhältnis zu Risiken und Deckungsumfang abgleichen		
6. Schadensabwicklung: Bewertungen sowie durchschnittliche Reaktionszeit prüfen		

Fazit: Cyberangriffe nehmen zu – Cyberversicherungen sind unabdingbar

Cyberangriffe nehmen zu – und das aus verschiedensten Gründen. Einerseits steigt die Menge an verfügbaren Daten im Netz. Dabei gilt: Je sensibler die Daten, desto mehr Geld lässt sich damit verdienen. Zudem erleichtert der stetige technologische Fortschritt Kriminellen den Zugang zu Wissen sowie Werkzeugen aus dem Darknet, um Cyberangriffe durchzuführen. Im Gegenzug dazu wachsen die Schwachstellen in Anwendungen durch steigende Komplexität und Verzahnung der IT. Außerdem steigt das Risiko durch Beschäftigte, die vermehrt im Homeoffice tätig sind und die Wartung ihrer Systeme selbständig übernehmen und nicht über alle Gefahren informiert sind.

Fest steht: Cyberangriffe werden weiter zunehmen, da sie äußerst lukrativ sind. Firewalls von Firmen weisen täglich im Schnitt 20.000 Angriffe ab – und es werden immer mehr. Um die Folgen zu begrenzen, sollten Unternehmen höchstmögliche Sicherheitsmaßnahmen vornehmen. Als Basis sind Konzepte sinnvoll, welche eine automatisierte sowie zentrale Verwaltung aller Clients ermöglichen und unternehmensspezifisch modular ergänzt werden können. Zusätzlich ist eine Cyberversicherung ratsam, die speziell an die Bedürfnisse des Unternehmens angepasst ist.

Über Aagon

„Manage any device in a connected world!" – Aagon entwickelt seit 30 Jahren Client-Management- und -Automation-Lösungen und ist der Spezialist für die Verwaltung von Endgeräten und die Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklungen, mehr als 20 Jahre Marktreife und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte perfekt auf Ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und ersten Einrichtung gehören deshalb zum Standard von Aagon. Ein umfassendes Verständnis von Kundenbedürfnissen und der ständige Kontakt zu unseren Kunden und Partnern ermöglichen Softwareentwicklung auf Augenhöhe. Webinare-on-Demand, zahlreiche Whitepaper und die beliebten Treffen zum Anwendertreffen an Standorten in ganz Deutschland sind nur drei Beispiele, wie nahe am Kunden ACMP wirklich entwickelt wird.

Aagon GmbH
Lange Wende 33
59494 Soest
Tel.: 02921 789 200
E-Mail: info@aagon.com
Web: www.aagon.com

GOLD
UNIFIED ENDPOINT MANAGEMENT
IP INSIDER AWARD 2023

techconsult
PUR 2023
Professional User Rating
★ 4-FACH ★
★ CHAMPION ★

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.