BLOCKY for VEEAM®

BACKUPS MIT APPLICATION-WHITELISTING VOR RANSOMWARE SCHÜTZEN

WHITEPAPER

APPLICATION WHITELISTING FÜR BACKUPS

Was ist Application-Whitelisting?

Wie funktioniert es?

Wer braucht es und warum?

ANGST VOR RANSOMWARE?

Application-Whitelisting ist das Schutzschild gegen Ransomware, die andere Abwehrmaßnahmen bereits durchbrochen hat.

INHALT

* 3 SUMMARY
* 4 DIE HERAUSFORDERUNG
* 5 MEHRSTUFIGER SCHUTZ
* 6 DAS OSI-MODELL
* 8 APPLICATION-WHITELISTING: PRO & KONTRA
* 10 WHITELISTING ALS ZUSÄTZLICHER SCHUTZ
* 11 LAST LINE OF DEFENSE
* 12 BLOCKY FOR VEEAM®
* 13 WHITELISTING: WER BRAUCHT ES?
* 14 CHECKLISTE AWL

SUMMARY

Cyberangriffe passieren auf mehreren Ebenen. Vor allem Ransomwareattacken schaffen es, oft sehr weit vorzudringen – ohne bemerkt zu werden. Als letzte Linie der Verteidigung gilt es, Backups vor Verschlüsselung zu schützen. Schreibzugriff auf das Backup-Volume sollte im Idealfall nur die Backup-Anwendung bekommen. Das stellt Application-Whitelisting sicher. Produkte wie BLOCKY for VEEAM® von GRAU DATA bieten Application-Whitelisting für einen bestimmten Einsatzzweck: Es schützt Backups vor Verschlüsselung durch Ransomware. Lernen Sie in diesem Whitepaper, wie Sie Ihre letzte Verteidigungslinie aufbauen.

VERTRAUEN IST DIE GRUNDLAGE

DIE HERAUSFORDERUNG

Mechanismen zum Schutz sensibler Daten und Programme umfassen eine Vielzahl an Maßnahmen. Das schwächste Glied der in jeder Verteidigungskette ist der Mensch. Trotz groß angelegter Awarenesskampagnen gehen viele Anwender sorglos mit vertraulichen Informationen um, veröffentlichen ihre Passwörter und ignorieren ungewöhnliches Verhalten ihres PC oder einer Software.

Darüber hinaus sollte auch jedes Unternehmen über eine umfassende und effektive IT-Sicherheitsstrategie verfügen. Dennoch haben viele Firmen veraltete und unzureichende Schutzmaßnahmen. Der Grund dafür sind die Kosten. Wirkungsvolle Sicherheitsmaßnahmen sind teuer, zeitaufwändig und erfordern Fachwissen. Die Umsetzung scheitert also meistens am zu kleinen Budget, zu hohem Zeitdruck und mangelnder Expertise.

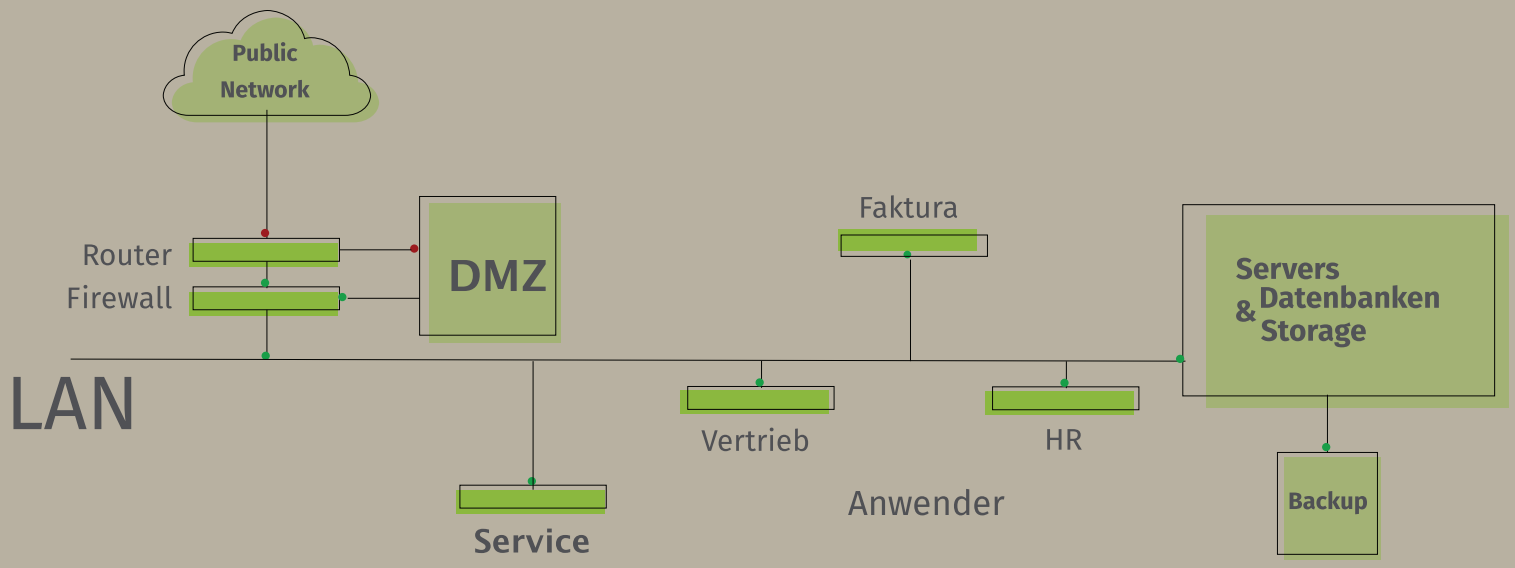
ANGRIFFE KÖNNEN SOWOHL VON INNEN ALS AUCH VON AUSSEN ERFOLGEN.

Der Sicherheitstacho der DTAG erfasst mit seiner Honeypotinfrastruktur weltweit bis zu 20.000 Cyberangriffe pro Minute. Laut einer Studie des Digitalverbandes Bitkom wurden 2018 in Deutschland 7 von 10 Unternehmen Opfer einer Cyberattacke, der entstandene Schaden betrug mehr als 40 Mrd. Euro. Das Bundesamt für Sicherheit in der IT (BSI) veröffentlicht jedes Jahr den Bericht zur Lage der IT-Sicherheit in Deutschland. Im letzten Jahr wurden 53% der gemeldeten Vorfälle durch Malware (Schadsoftware) verursacht. Dabei betrug der Anteil auf Erpressung abzielender Schadsoftware (Ransomware) 13%.

Ransomware stellt eine besondere Herausforderung an die Datensicherheit dar. IT-Sicherheitsexperten sind sich einig, dass es extrem aufwändig bis unmöglich ist, durch Ransomware verschlüsselte Daten ohne den Schlüssel des Erpressers wieder zu entschlüsseln.

Typische externe Angriffsszenarien sind kompromittierte Emails oder Webseiten und gezielte Angriffe, die Schwachstellen im Netzwerk oder in Programmen ausnutzen. Bei internen Angriffsszenarien sind immer Mitarbeiter involviert, wobei nicht immer zwingend ein Vorsatz bestehen muss.

Sind die Daten, eine Anwendung oder das Netzwerk kompromittiert, heißt der letzte Ausweg Backup. Doch was ist, wenn auch diese kompromittiert sind? Schützen Sie Ihre Backups wirkungsvoll vor Angriffen und Verschlüsselung! In diesem Whitepaper erfahren Sie, wie Unternehmen ihre IT mehrstufig schützen können und warum Backups zusätzlich mit Application-Whitelisting abgesichert werden müssen.



Mehrstufiger Schutz

Auf Grund der vielen möglichen Angriffsszenarien muss auch der Schutz mehrstufig sein:

- Netzübergänge (Perimeter) müssen über eine Technologie- und Hersteller-Redundanz verfügen.
- Dienste, die von außen erreichbar sind, müssen in einer entmilitarisierten Zone (DMZ) betrieben werden.
- Daten müssen klassifiziert (z. B. nach dem Need-to-Know-Prinzip) und interne Netze entsprechend segmentiert werden.
- Endpoints wie PCs oder Laptops, sollten über zusätzliche Schutzmaßnahmen verfügen.

DAS OSI-MODELL

DAS OSI-7-SCHICHTEN-MODELL IST DAS REFERENZMODELL FÜR DEN NETZWERKSTACK

Eine IT-Infrastruktur besteht aus physischen und virtuellen Schichten (Layern). Jede Schicht ist auf besondere Weise angreifbar.

Ein besonderes Risiko stellen so genannte Zero-Day-Angriffe dar. Bei diesen Angriffen nutzen die Angreifer noch unbekannte Schwachstellen in Hard- oder Software aus.

Die meisten am Markt erhältlichen Schutzmaßnahmen basieren auf Black-Listing. Beim Black-Listing werden als schädlich eingestufte oder unerwünschte Anwendungen, Email-Absender, Websites oder Dateiformate blockiert. Firewalls, Viren, URL- und Malwarescanner, welche auf dieser Technologie basieren, können nur vor etwas schützen, was bereits bekannt und signiert ist. Damit fallen sämtliche Zero-Day-Angriffe, neue Malware und Computerviren durch das Raster.

Moderne Schutzmaßnahmen arbeiten deshalb mit White-Listing. Bei dieser Technologie wird alles blockiert, was nicht als vertrauenswürdig erkannt und ausdrücklich erwünscht ist. Dieser Ansatz wird als der Sicherere eingestuft. White-Listing kann auch vor noch unbekannten Angriffsszenarien, den so genannten Zero-Day-Exploits, schützen. Auch macht die zunehmende Anzahl an Bedrohungen es zunehmend schwerer, die dem Black-Listing zugrundeliegenden Datenbanken auf aktuellem Stand zu halten.

Die empfohlenen Maßnahmen für unterschiedlichen Layer des Open-Systems-Interconnection (OSI)-Modells unterscheiden sich nach ihrem Einsatzweck.

Application-Whitelisting setzt auf der Anwendungsebene an. Die Anwendungsebene baut auf der TCP/IP-Protokollfamilie auf und ist die oberste Schicht des OSI-7-Schichten-Modells.

WIE WIRKT APPLICATION-WHITELISTING?

Jede Anwendung, jede Datei, jedes Verhalten hat eine einzigartige Signatur, die in einer Datenbank hinterlegt ist. Bei der Integritätsprüfung wird verglichen, ob es sich um einen autorisierten Zugriff einer erlaubten Anwendung handelt. Entspricht das Anwendungsmuster nicht der hinterlegten Signatur, wird der Zugriff blockiert.

Dieses Vorgehen ist nicht nur effektiv, es ist auch sehr effizient. In der Praxis ist die Anzahl erlaubter Anwendungen wesentlich geringer als die Anzahl der als schädlich oder unerwünscht eingestuften Programme.

Auf Whitelisting basierende Schutzmaßnahmen reagieren also nicht nur schneller. Sie sind auch wesentlich schlanker als ihre auf Black-Listing aufsetzenden Pendants. Das spart Platz, Zeit und Kosten, weil weniger leistungsfähige Systeme benötigt werden.

Application-Whitelisting schützt wirkungsvoll vor Viren und Malware, an deren Erkennung herkömmliche Maßnahmen scheitern. Schutzmaßnahmen auf Basis von White-Listing erhöhen die IT-Sicherheit. Dennoch sind sie bisher wenig weit verbreitet.

PRO

Was für den Einsatz von Application-Whitelisting spricht:

- Schützt wirkungsvoll vor Angriffen
- Schützt auch vor Zero-Day-Szenarien
- Ist schnell und effizient
- Beugt ungewöhnlichen Verhaltensmustern vor
- Eignet sich für alle Unternehmen – egal welcher Branche oder Größe

KONTRA

Woran die Verbreitung bisher scheitert:

- Hoher Implementierungsaufwand
- Zeitaufwendige Pflege
- Setzt zentrale Datenbanken voraus

MIT BLOCKY FOR VEEAM® ALS LETZTE VERTEIDIGUNGSLINIE BLEIBEN IHRE DATEN JEDERZEIT SICHER & GESCHÜTZT.

Im Vorteil sind auf bestimmte Anwendungsfälle spezialisierte Lösungen, die sich transparent in bestehende Infrastruktur integrieren. BLOCKY for VEEAM® ist eine solche Lösung.

WHITELISTING

ALS ZUSÄTZLICHER SCHUTZ

„Es gibt keine Silberkugel in der Informationssicherheit. Aber korrekt eingesetztes White-Listing bietet außerordentlichen Schutz vor Zero-Day- und gezielten Angriffen.“ – The Power of Whitelisting, Neil MacDonald, Gartner

IT-Sicherheit ist alles andere als schwarz-weiß. Für einen umfassenden Schutz kommt es also auf die wirkungsvolle Kombination verschiedener Maßnahmen an. Weder kann eine Firewall alleine ein Unternehmen vor allen Angriffsszenarien schützen, noch vermag es eine einzelne Antiviren-Software. Maßnahmen sollten immer sowohl auf ihren Einsatzort als auch auf den Zweck ausgesucht und abgestimmt werden.

Firmen mit einer Backup-Strategie sind weniger anfällig für Erpressungsversuche durch Ransomware. Laut einer Studie des Uptime Institute sind allerdings nur 68% der Unternehmen in der Lage, kurzfristig ihre Daten wiederherzustellen.

Backups sollten täglich inkrementell angefertigt werden. Außerdem empfehlen wir, die Daten einmal wöchentlich auf ein Medium zu kopieren, welches offline an einem externen Ort gelagert wird. Regelmäßig sollten auch Vollbackups inklusive der Server für ein Bare Metal Restore (BMR) gemacht werden.

Zwei Dinge sind besonders wichtig im Ransomwareschutz:

- aktuelle Kopien der Daten mindestens Offsite, besser zusätzlich auch Offline vorzuhalten
- die Fähigkeit, anomale Prozesse sofort zu erkennen und abzuwehren

Dieses Vorgehen lässt sich ganz einfach mit der 3-2-1-Regel merken und umsetzen: Machen Sie drei Kopien der Daten auf zwei verschiedenen Medientypen und speichern Sie je eine Kopie Offsite und Offline.

Doch die Angriffsszenarien werden immer komplexer: Mit Samas hat es eine Ransomware erstmals gezielt auf Backups abgesehen – genau gesagt auf Veeam-Backups. Während sich Ransomware bisher damit begnügte, Volume Shadow Copies (Snapshots) zu löschen, verschlüsselt Samas über einen längeren Zeitraum unbemerkt Backupdaten. Das Lösegeld wird erst nach 30 Tagen oder später eingefordert. Die Angreifer kalkulieren mit der Sparsamkeit der Unternehmen: Aus Kosten- und Platzgründen werden Backups oft innerhalb eines Monats vollständig überschrieben.

Moderne Backup-Lösungen bieten automatisiert schnelles Backup-to-Disk, eine BMR-Integration, das Erstellen mehrerer Datenkopien und die Sicherung auf ein Offline-Medium wie Tape sowie in die Cloud (offsite). Sie können sogar vor Ransomware-Gefahr warnen, wenn untypische Backupverläufe erkannt werden. Die von physischen Medien bekannte WORM-Technologie wurde in digitale Prozesse übernommen.

FIRMEN MIT EINER BACKUP-STRATEGIE SIND WENIGER ANFÄLLIG FÜR ERPRESSUNGSVERSUCHE DURCH RANSOMWARE.

LAST LINE OF DEFENSE

WORM-Technologie existiert schon seit vielen Jahren. Mit WORM wird einmalig das Schreiben und unbegrenzte Lesevorgänge erlaubt. Die Veränderung einer geschriebenen Datei ist ausgeschlossen. WORM hat seinen Ursprung in physischen Datenträgern wie CDs oder DVDs, die zwar beschrieben, jedoch anschließend nicht mehr verändert werden konnten. Festplatten und wiederbeschreibbare CDs bzw. DVDs stellten neue Anforderungen.

Eine dedizierte Software-Schicht im Betriebssystemkern kontrolliert das Lesen und vor allem das Schreiben von Daten auf der Festplatte. Filter steuern sämtliche schreibenden Zugriffe auf das Dateisystem. Dabei werden Schreibvorgänge ausschließlich für neue Dateien zugelassen. Ein nachträgliches Verändern vorhandener Daten wird verhindert. Damit wird zwar das Verschlüsseln von Daten unterbunden, es stellt die Unternehmen aber vor eine ganz andere Herausforderung.

Änderungen am originalen Datenbestand müssen auch im Backup abgebildet werden. Backup-Lösungen müssen also Daten auch verändern oder löschen können. Auch muss sichergestellt werden, dass Daten nach einer gewissen Vorhaltezeit auch im Backup gelöscht werden können. Andernfalls würde das einen immensen Verschleiß an physischen Datenträgern nach sich ziehen.

Dazu wurde das Software-WORM um die Application-Whitelisting erweitert. So wird der Backup-Lösung das Verändern der Daten gestattet.

GRAU DATA hat ein solches WORM-System für den Schutz von lokalen Backup-Repositories entwickelt, das beispielsweise für Veeam als „Blocky for Veeam“ erhältlich ist.

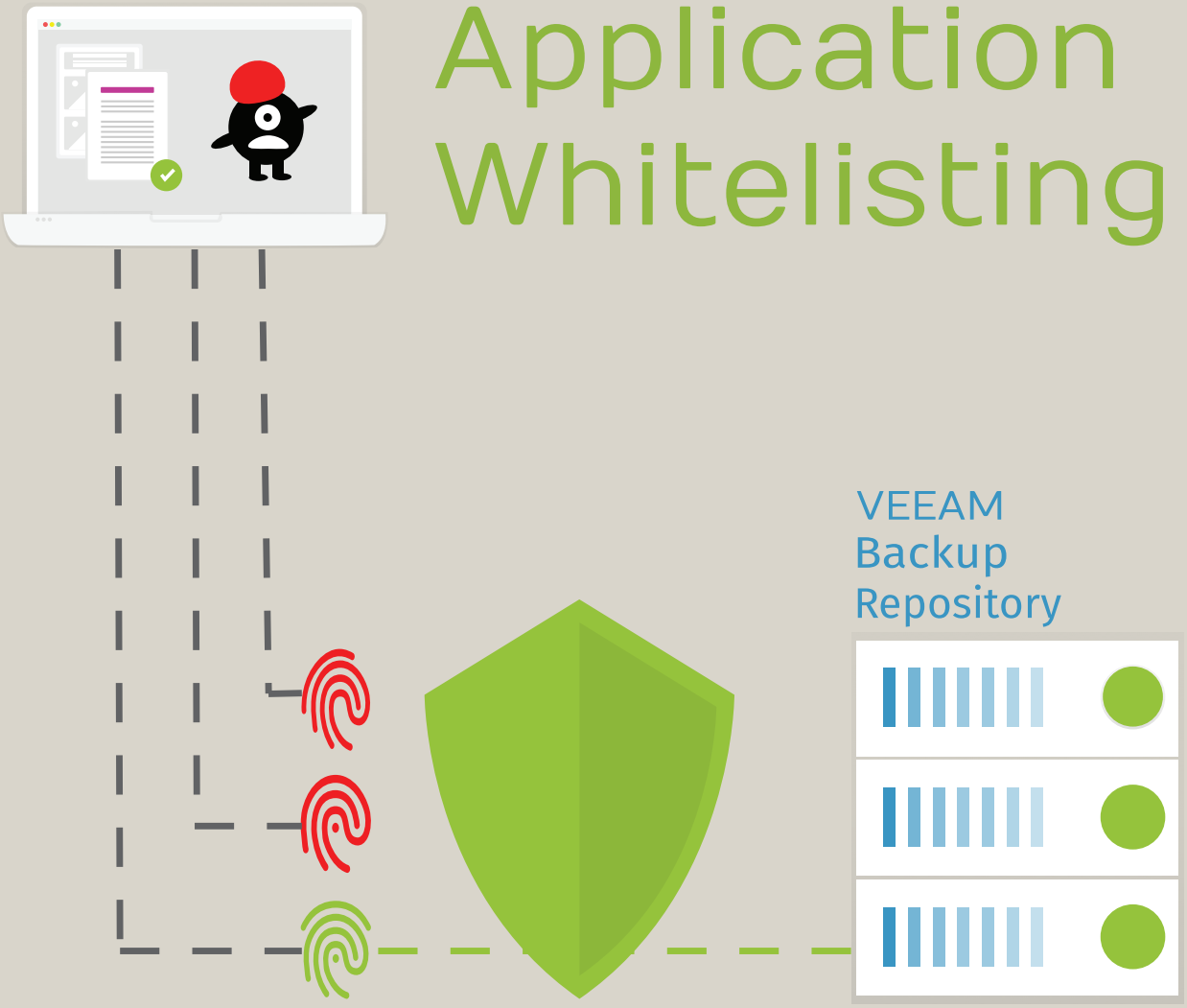
BLOCKY for VEEAM® verhindert Änderungen und schützt Backupdaten vor Verschlüsselung durch Ransomware wie Samas. Das integrierte White-Listing stellt sicher, dass nur eine autorisierte Backup-Anwendung Schreibzugriff auf das Backup-Volume hat. Dazu muss die Backup-Anwendung sich mit ihrem Fingerabdruck ausweisen: nur wenn der Fingerabdruck mit der zuvor hinterlegten Referenz übereinstimmt, lässt die Filterschicht den schreibenden Zugriff der Backup-Anwendung auf die Daten zu. Alle anderen Zugriffsversuche, insbesondere durch Schadprogramme wie Ransomware, werden durch das Whitelisting blockiert.

Unautorisierte Zugriffe werden außerdem geloggt und der Administrator enachrichtigt.

Voraussetzung hierfür ist ein lokales Backup-Repository am Backup-Server – entweder direkt auf dem Server bei Standalone-Installation oder separiert auf einem dedizierten Proxy-Server in verteilten Umgebungen. Das Repository liegt auf einem lokalen Block-Device, etwa als interne Disk, FC-LUN, iSCSI-LUN, welches aus Sicht des Windows-Betriebssystems als lokales Volume konfiguriert wird. Dabei werden sowohl NTFS- als auch ReFS-Dateisysteme unterstützt, was insbesondere für kritische Umgebungen eine zusätzliche Resilienz garantiert.

BLOCKY FOR VEEAM®

WIRKUNGSWEISE



WHITELISTING

WER BRAUCHT ES?

Application-Whitelisting ist Bestandteil vieler Betriebssysteme. Vor allem Remote-Desktop-Infrastrukturen profitieren von der vergleichsweise einfachen Verwaltung bei nur geringen Kosten.

Backup-Lösungen verfügen selbst nicht über die Whitelisting-Technologie. Hier muß über den Einsatz von Lösungen so genannter Drittanbieter (Third-Party-Solution). Bei der Auswahl sollte darauf geachtet werden, dass diese Lösungen robust sind und sich zentral administrieren lassen. Vorher sollte die Umgebung, in der das Application-Whitelisting eingesetzt werden soll, eingehend evaluiert werden. Es ist einfacher, das Application Whitelisting auf zentral administrierten Systemen zu betreiben. Besonders empfehlenswert ist der Einsatz bei erhöhtem Sicherheitsbedarf, u. a. in kritischen Infrastrukturen oder Banken und Versicherungen.

Risikobetrachtungen helfen Organisationen, die Vorteile von zusätzlichen Maßnahmen wie dem Application-Whitelisting zu bewerten.

Firmen, die nicht über ausreichend geschultes Personal verfügen, sollten den Einsatz externer Fachkräfte in ihre Betrachtungen einfließen lassen. Unternehmen kleinerer und mittlerer Größe (KMU) wird ohnehin empfohlen, die Betreuung ihrer IT an geeignete Partner auszulagern.

Jedes Unternehmen, egal welcher Größe, sollte Application-Whitelisting wenigstens in einem Monitoring-Modus einsetzen.

Der Einastz von Application-Whitelisting ist in diesen drei Szenarien besonders empfohlen:

1. Zentral verwaltete Server (Hosts), die mit anderen Computern verbunden sind
2. Hosts in kritischen Infrastrukturen oder bei Banken und Versicherungen (high-risk environment)
3. Auf Geräten oder an Standorten, an denen die Anwender keine Adminrechte haben

Beim Einsatz von Application-Whitelisting werden ausschließlich autorisierten Anwendungen Zugriffsrechte eingeräumt. Das verringert das Risiko, welches von vor allem unbekannten Schwachstellen ausgeht. Unternehmen müssen im Vorfeld evaluieren, welche Programme welche Rechte erhalten sollen.

Application-Whitelisting ist eine Technologie, welche die Sicherheit Ihrer Daten erhöht und Ihr Unternehmen vor Malware schützt. Zusammen mit klassischen Schutzmechanismen bewahrt es Ihre Daten und die IT-Infrastruktur davor, kompromittiert zu werden.

Diese Checkliste hilft bei der Implementation von Application-Whitelisting (AWL).

1. Identifizieren Sie, was von AWL überwacht werden soll. Beziehen Sie Betriebssysteme, Anwendungen und Schittstellen zu anderen integrierten Systemen in die Betrachtung ein.
2. Entscheiden Sie, ob unautorisierte Anwendungen rigoros geblockt oder nur überwacht werden sollen.
3. Überprüfen Sie, welche Systeme bereits mit der Whitelisting-Technologie ausgestattet sind und wo Sie Produkte von Drittanbietern dazukaufen müssen.
4. Achten Sie bei Fremdsystemen auf eine effektive Systemarchitektur und die Möglichkeit zu einer nahtlosen Integration in die bestehende Systemlandschaft.
5. Bevor Sie die AWL-Lösung installieren, prüfen Sie das System auf Malware.
6. Testen Sie die AWL-Technologie im Monitoring-Modus, um sicherzustellen, dass sie allen Anforderungen entspricht.
7. Testen Sie außerdem, ob die AWL-Lösung die richtigen Anwendungen erlaubt und unautorisierte Software blockt.
8. Stellen Sie ausreichend geschultes Personal ein oder beauftragen Sie einen geeigneten Partner mit der Betreuung des Systems.

DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI) EMPFIEHLT ZUM SCHUTZ VOR ANGRIFFEN DURCH RANSOMWARE WIE EMOTET & CO DEN EINSATZ VON APPLICATION WHITELISTING.

BLOCKY for VEEAM®

GRAU DATA
YOUR DATA. YOUR CONTROL

GRAU DATA GmbH
Marie-Curie-Straße 19
73529 Schwäbisch Gmünd
Deutschland

Partnervertrieb

cristie.partners

Cristie Data GmbH
Nordring 53-55
63843 Niedernberg
Deutschland

Kontakt

team@cristie.partners
+49 6028 979 55 55

www.blockyforveeam.de