DriveLock
securing your digital tomorrow

DriveLock Vulnerability Management

Whitepaper

DriveLock
securing your digital tomorrow

Inhalt

Management Summary

In Zeiten der digitalen Transformation hängt Ihr Erfolg davon ab, wie Sie Menschen, Unternehmen und Dienste zuverlässig vor Cyber-Angriffen und dem Verlust sensibler Daten schützen können. Mit der Omnipräsenz der Informationstechnologie und ihren Abhängigkeiten sehen sich Organisationen mit einer Zunahme der Anzahl und Schwere von Bedrohungen konfrontiert. Dies hat negative Auswirkungen auf den Betrieb, die Vermögenswerte und die Mitarbeiter. Angesichts des potenziellen Schadens, der durch menschliches Versagen und gezielte Cyber-Angriffe und andere Bedrohungen entstehen kann, muss eine Organisation mehr Gewicht auf das Management der mit ihren Systemen verbundenen Schwachstellen und Risiken legen.

Angreifer nutzen Schwachstellen oder Schwächen in der Software aus, um die Kontrolle über Computersysteme zu erlangen, sensible Informationen zu stehlen und den Betrieb zu unterbrechen. Schwachstellen können in Betriebssystemkomponenten oder Softwareanwendungen liegen. IT-Manager müssen die mit diesen Schwachstellen verbundenen Risiken identifizieren und kontrollieren.

Die Verwaltung der unzähligen Konfigurationen innerhalb der Systemkomponenten ist mit manuellen Methoden zu einer unmöglichen Aufgabe geworden.

Wenn möglich, suchen Organisationen nach automatisierten Lösungen, die Kosten senken, die Effizienz steigern und die Zuverlässigkeit der Cybersicherheitsbemühungen langfristig verbessern können.

Es ist wichtig, Schwachstellen zu identifizieren, die sofortige Aufmerksamkeit erfordern. Ein automatisiertes, risikobasiertes Schwachstellenmanagement hilft, eine große Anzahl von Schwachstellen zu bewältigen und den Fokus auf schnelles und effektives Handeln aufrechtzuerhalten.

Die DriveLock Vulnerability Management Lösung identifiziert Schwachstellen auf Endpunkten, macht sie sichtbar und verhindert so potenzielle Malware-Angriffe. IT-Administratoren können die mit Schwachstellen verbundenen Risiken erkennen und kontrollieren.

Ständig sich ändernde IT-Landschaften und sich entwickelnde Cyber-Bedrohungen machen regelmäßige Scans und Konformitätsprüfungen erforderlich, um Unternehmen vor Cyber-Angriffen zu schützen. Damit Ihre Unternehmensumgebung sicher bleibt, benötigen Sie eine Lösung für das Schwachstellenmanagement, die Ihnen einen vollständigen Einblick in Ihre Angriffsfläche bietet, damit Sie Ihr Cyberrisiko verwalten und messen können. DriveLock Vulnerability Management ist Teil der DriveLock Zero Trust Platform und bietet Ihnen einen umfassenden Überblick über Ihre Infrastruktur.

Bedrohungslage

Cyberangriffe und Datenschutzverletzungen können durch eine Vielzahl von Dingen verursacht werden. Im Fall von Equifax [ZDNet] beispielsweise hatte es schwerwiegende Folgen, dass eine bekannte Schwachstelle, die sich auf die verwendete Software oder die verwendeten Bibliotheken auswirken kann, nicht innerhalb einer angemessenen Zeitspanne behoben wurde. Der „Data Breach" bei Equifax ist ein typisches Beispiel für einen bedeutenden Cyberangriff, bei dem persönliche Daten von fast 150 Millionen Kunden offengelegt wurden [ZDNet].

In anderen Fällen können ungesicherte, dem Internet ausgesetzte Daten ein Problem darstellen. Zero-Day-Schwachstellen können nach Belieben ausgenutzt werden, bevor Korrekturen verfügbar sind, oder in einigen der schlimmsten Fälle kann eine Organisation oder eine Einzelperson von staatlich finanzierten Advanced Persistent Threat (APT)-Gruppen ins Visier genommen werden, die über beträchtliche Ressourcen und Werkzeuge verfügen.

Tatsächlich reicht manchmal ein einziger anfälliger Endpunkt, ein Netzwerk, ein Server oder eine Anwendung aus, um Millionen von Menschen zu beeinträchtigen. Shellshock, Heartbleed, Poodle und EternalBlue sind nur einige der berüchtigten Schwachstellen, die dem Datendiebstahl durch Malware und anderen Angriffen Tür und Tor geöffnet haben. Es gibt unzählige weitere - im Jahr 2017 gab es 1.522 öffentlich gemeldete Schwachstellen. Die Zero Day Initiative [ZDI] hat aufgedeckt, dass 929 davon als "kritisch" oder "hoch" eingestuft wurden [ZDI].

Kosten für Unternehmen

Neben der Bedrohungslandschaft stellt sich auch die Frage nach den Kosten für Unternehmen, die einem Angriff oder einer Datenverletzung ausgesetzt sind. Cyberkriminalität ist ein profitables Geschäft, mit relativ geringen Risiken im Vergleich zu anderen Formen der Kriminalität.

279 Days Time to identify and contain a breach (MTTD 206, MTTR 73)	**$3.9 M ($4.8M Germany)** Average total cost of data breaches	**+27 % ($4.45M vs. $3.5M)** Breaches caused by a malicious attack were more costly than breaches caused by human error	**51 %** Malicious attacks were the most common and most expensive root cause of breaches

Das Ponemon Institute hat einen Lagebericht erstellt. Im Jahr 2019 dauerte es im Durchschnitt 279 Tage, bis ein Verstoß entdeckt und eingedämmt wurde. Je schneller eine Datenschutzverletzung nach einem Cyberangriff erkannt und eingedämmt werden kann, desto geringer sind die Kosten. Die durchschnittlichen Gesamtkosten eines "Datenverstoßes" belaufen sich weltweit auf 3,9 Millionen US-Dollar, in Deutschland sogar 4,08 Millionen US$.

Herausforderung

Angreifer nutzen Schwachstellen (vulnerabilities) oder andere Schwachpunkte (weaknesses) in Software aus, um die Kontrolle über Computersysteme zu erlangen, sensible Informationen zu stehlen und Unterbrechungen von Diensten zu verursachen. Schwachstellen können in den Betriebssystemkomponenten oder Softwareanwendungen liegen. IT-Administratoren müssen die mit diesen Schwachstellen verbundenen Risiken identifizieren und verwalten. Bei Organisationen, die nicht nach Schwachstellen suchen und entdeckte Mängel nicht proaktiv angehen, ist die Wahrscheinlichkeit hoch, dass ihre Computersysteme kompromittiert werden.

Vulnerability Management

Vulnerability Management-Produkte können sehr komplex in der Anwendung sein, viel Netzwerkbandbreite beanspruchen und Systemressourcen verbrauchen. Infolgedessen zögern Unternehmen, tägliche Schwachstellen-Scans durchzuführen. Stattdessen werden die Scans wöchentlich, monatlich oder vierteljährlich durchgeführt. Und selbst nachdem ein Scan abgeschlossen ist, stehen IT-Abteilungen vor der Frage, wie sich Schwachstellen leicht beheben lassen. Das Schwachstellen-Management bewertet kontinuierlich Risiken, und durch Automatisierung wird es zur täglichen Routine.

Ein effektives risikobasiertes Schwachstellenmanagement erfordert einen klar definierten Prozess.

Eine Schwachstelle ist eine Sicherheitslücke in einem Informationssystem, in Systemsicherheitsverfahren, in internen Kontrollen oder in der Implementierung, die von einer Bedrohungsquelle ausgenutzt oder ausgelöst werden könnte. Hinweis: Der Begriff der Schwachstelle ist ein Synonym für Mangel. Eine Schwachstelle kann zu Sicherheits- und/oder Datenschutzrisiken führen [NIST].

Die NATIONAL VULNERABILITY DATABASE (NVD) **[NIST NVD]** ist das Repository der US-Regierung für standardbasierte Schwachstellenmanagement-Daten, die durch das Security Content Automation Protocol (SCAP) repräsentiert werden. Diese Daten ermöglichen die Automatisierung des Vulnerabilty Managements, der Sicherheitsmessung und der Einhaltung von Vorschriften.

Automationstools

Wenn möglich, versuchen Organisationen, die das System beschreibenden Daten zu normalisieren, so dass die verschiedenen Überwachungsergebnisse in konsistenter Weise kombiniert, korreliert, analysiert und berichtet werden können. **Die Verwaltung der unzähligen Konfigurationen innerhalb der Systemkomponenten mit manuellen Methoden ist zu einer unmöglichen Aufgabe geworden**. Wann immer möglich, suchen Organisationen nach automatisierten Lösungen, die Kosten senken, die Effizienz steigern und die Zuverlässigkeit der Cybersicherheitsbemühungen langfristig verbessern können. Die Behörden empfehlen standardisierte Werkzeuge für die Automatisierung [NIST P21]. Für Organisationen mit einer großen Anzahl von Komponenten besteht die einzige praktische und effektive Lösung darin, automatisierte Lösungen zu verwenden, die standardisierte Berichtsmethoden wie SCAP verwenden.

Standardisierung mit SCAP

Beim Kauf von Lösungen sind Organisationen gut beraten, SCAP-validierte Lösungen in die engere Wahl zu nehmen. SCAP bedeutet Security Content Automation Protocol (Protokoll zur Automatisierung von Sicherheitsinhalten). SCAP bietet eine gemeinsame Sprache zur Beschreibung von Schwachstellen, Fehlkonfigurationen und Produkten. Für Organisationen, die einen zuverlässigen Weg suchen, um den Sicherheitsstand der Unternehmensarchitektur innerhalb der Organisation zu vermitteln, ist dies ein naheliegender Ansatzpunkt [NIST-SCAP]. Das Security Content Automation Protocol (SCAP) umfasst eine Reihe von Spezifikationen, die das Format und die Nomenklatur standardisieren, mit denen Informationen über Software-Fehler und sichere Konfigurationen übermittelt werden können.

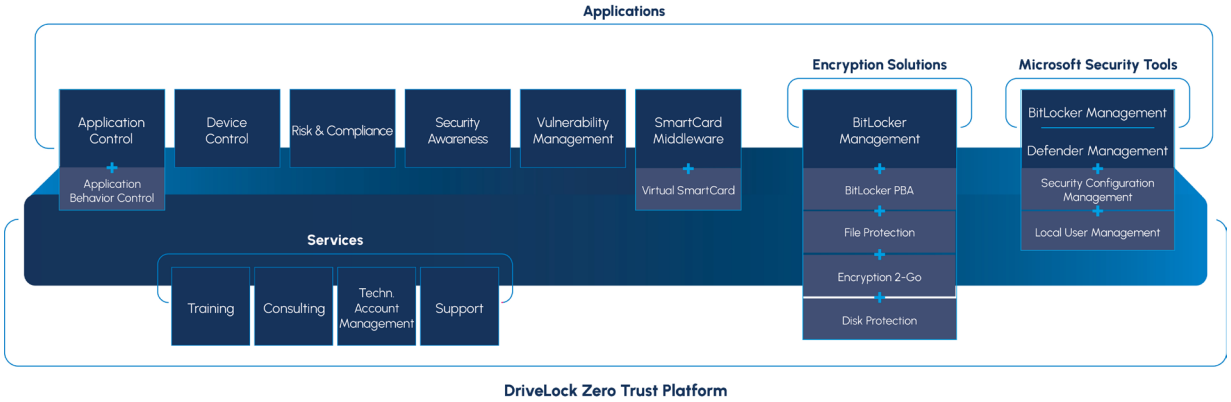
Beispielsweise ist das Common Vulnerability Scoring System (CVSS) eine Spezifikation innerhalb von SCAP, die einen offenen Rahmen für die Kommunikation der Merkmale von Softwareschwachstellen und für die Berechnung ihres relativen Schweregrads bietet. Das CVSS bietet eine Möglichkeit, die Hauptmerkmale einer Schwachstelle zu erfassen und eine numerische Bewertung zu erstellen, die den Schweregrad der Schwachstelle widerspiegelt. Die numerische Bewertung kann dann in eine qualitative Darstellung (z. B. niedrig, mittel, hoch und kritisch) übersetzt werden. Dies dient der Veranschaulichung und hilft bei der genauen Bewertung und Priorisierung von Schwachstellenmanagementprozessen [FIRST]. CVSS ist ein öffentlicher Standard, der von Organisationen weltweit verwendet wird. CVSS-Bewertungen können zur Verbesserung der Sicherheitslage („Security Postures") verwendet werden.

OVAL® ist eine Marke des US-Heimatschutzministeriums (Department of Homeland Security, DHS). Open Vulnerability and Assessment Language (OVAL), ist eine Sprache zur Darstellung von Systemkonfigurationsinformationen, zur Bewertung des Maschinenzustands und zur Meldung von Bewertungsergebnissen. **OVAL®** ist international und für die Öffentlichkeit frei verfügbar. **OVAL®** ist eine Initiative der Informationssicherheits-Community zur Standardisierung der Bewertung und Berichterstattung über den Maschinenzustand von Computersystemen. OVAL umfasst eine Sprache zur Kodierung von Systemdetails und eine Reihe von Repositories, die in der gesamten Community gehalten werden.

CVE ist eine vom US-Heimatschutzministerium gesponserte und eingetragene Marke der MITRE Corporation. CVE ist eine SCAP-Spezifikation, die eindeutige gemeinsame Namen für öffentlich bekannte Schwachstellen in Informationssystemen [Mitre] bereitstellt. Gemäß der Empfehlung des NIST muss eine Sicherheitssoftware die Unterstützung für Common Vulnerabilities and Exposures (CVE) enthalten.

Der DriveLock Vulnerability Scanner

Ständig sich ändernde IT-Landschaften und sich entwickelnde Cyber-Bedrohungen machen regelmäßige Scans und Konformitätsprüfungen erforderlich, um Unternehmen vor Cyber-Angriffen zu schützen. Damit Ihre Unternehmensumgebung sicher bleibt, benötigen Sie eine Schwachstellen-management-Lösung, die Ihnen einen vollständigen Überblick über Ihre Angriffsfläche bietet, damit Sie Ihr Cyberrisiko verwalten und messen können. DriveLock Vulnerability Management ist Teil der DriveLock Zero Trust Platform und bietet Ihnen einen umfassenden Überblick Ihrer Infrastruktur. Sie erhalten eine kontinuierliche Bewertung Ihrer Sicherheits- und Compliance-Position, so dass Sie unbekannte Assets und Schwachstellen entdecken und Schwachstellen priorisieren können, um Ihr Cyberrisiko zu minimieren und Verletzungen zu verhindern. DriveLock Vulnerability Management (VM) ist sowohl „on premise" als auch als Cloud-basierter Dienst verfügbar, der einen automatischen täglichen Schwachstellen-Scan durchführt. Unternehmen können ihre Bedrohungen und Schwachstellenrisiken schnell erkennen. DriveLock VM bietet einen kontinuierlichen Einblick in IT-Systeme. Es baut auf einer bewährten SCAP-Feed-Datenbank mit umfassender Schwachstellenabdeckung auf. Und unter Verwendung eines OVAL-Scanners enthält es eine Sprache zur Kodierung von Systemdetails. Der DriveLock-Schwachstellen-Scanner sucht automatisch nach Schwachstellen in einem Computersystem. Er tut dies auf planmäßiger, ad-hoc oder - falls gewünscht - regelmäßiger Basis. DriveLock verwendet eine Schwachstellen-Datenbank, die mehrmals täglich aktualisiert wird.



Vorteile

- Kontinuierliche Bewertung von Schwachstellen und der aktuellen Sicherheitslage
- Immer wissen, wenn Änderungen Ihre Angriffsfläche verändern
- Umfassender Überblick über Ihre IT-Infrastruktur
- Konzentrieren Sie sich auf das Wesentliche, indem Sie schnell herausfinden, welche Schwachstellen für die größte Risikoreduzierung vorrangig zu behandeln sind.
- Gewährleistung der Sicherheit und Nachweis der Einhaltung von Vorschriften mit Hilfe spezifischer Metriken, die den Status klar kommunizieren
- Standardisierung durch SCAP-validierte Lösung
- Skalierbare Lösung für kleine, mittlere und große Unternehmen
- Maßgeschneiderte Implementierungs- und Hosting-Modelle für Ihr Unternehmen

Schwerpunkt ist es, Kunden dabei zu helfen, das Schwachstellenrisiko zu verstehen, dem ihr Unternehmen ausgesetzt ist.

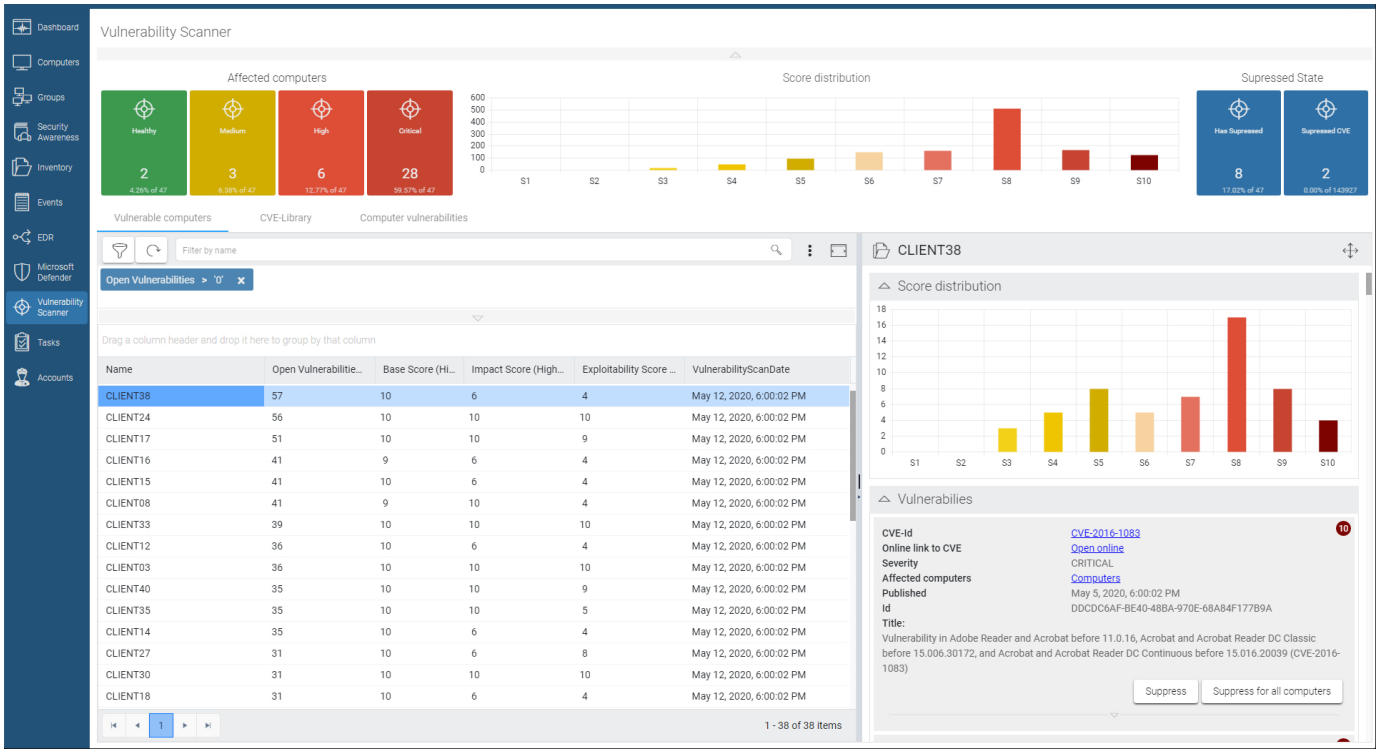
Funktionen & Leistungsmerkmale

- Umfassende Schwachstellen-Datenbank mit 115.000 Definitionen für insgesamt ca. 140.000 CVEs
- Bietet tiefe Einblicke durch kontinuierliches Monitoring.
- Stellt fest, ob eine Schwachstelle ausnutzbar ist.
- Bietet einen Überblick über alle Schwachstellen mit unterschiedlichen Scores bei den Endpunkten.
- Führt Scans automatisch, geplant oder manuell aus.
- Unterdrückt Schwachstellen, die nicht von Interesse sind.
- Neu erstelltes Dashboard, Widgets und spezifische Ansicht im DriveLock Operations Center
- Stündliche Aktualisierung der internen Bedrohungsdatenbank
- Folgt dem NIST-Standard durch die Verwendung von SCAP und erkannten CVEs mit CVSS-Scores
- Läuft unter Windows 10, 8, 7 und Windows Server.
- Mandantenfähigkeit, Mehrbenutzer- und rollenbasierter Zugriff

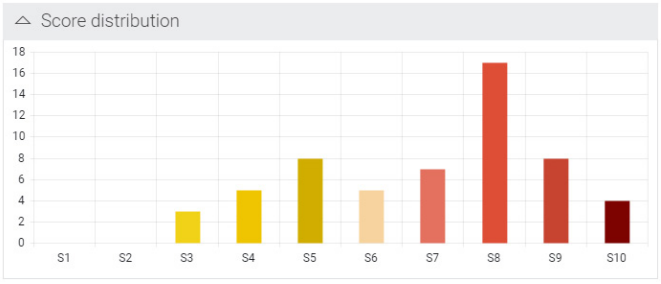
Monitoring & Reports

Dank der DriveLock-Schwachstellendatenbank erkennt der Agent Schwachstellen auf den Endpunkten und verhindert Malware-Angriffe.

IT-Administratoren können die mit Schwachstellen verbundenen Risiken erkennen und kontrollieren. Die gefundenen Ergebnisse werden in einer separaten Ansicht im DriveLock Operations Center (DOC) angezeigt. Der Schwachstellen-Scanner findet fehlende Patches, veraltete Softwareprogramme oder Bibliotheken mit bekannten Schwachstellen. Die verwendete Datenbank und die einzelnen Schwachstellen werden vom National Institute of Standards and Technology (NIST) und vom US-CERT verwaltet und aktualisiert. Es bewertet nach Schweregrad, Eintrittswahrscheinlichkeit und Auswirkung.



Das DriveLock Operations Center zeigt alle Informationen an und stellt Filter, Gruppierungen und sogar Berichte zur Verfügung. Dies ermöglicht eine wesentlich detailliertere und vor allem genauere Beurteilung der Sicherheitslage in Ihrem Unternehmen. Schwachstellen, die für Ihr Unternehmen nicht relevant sind oder für akzeptabel befunden werden, können unterdrückt werden. Dies ist eine wichtige Funktion, damit sich Analysten auf die relevanten Bedrohungen konzentrieren können. Ansichten (Views) zeigen die Gesamtzahl der gefundenen Schwachstellen auf allen Geräten in Ihrer Umgebung und klassifizieren den Schweregrad der Schwachstellen im Bereich Schwachstellenstatistik als niedrig, mittel, hoch und kritisch.
Wenn Sie auf einen Fensterbereich klicken, werden die entsprechenden Endpunkte angezeigt und weitere Details aufgelistet.



- **Identifizieren Sie Schwachstellen in Ihrem Umfeld.**
- **Beurteilen Sie, wie kritisch die gefundenen Schwachstellen sind.**
- **Schneller Blick auf mögliche Schwachstellen auf High-Level Ebene**

Sie erhalten nahezu in Echtzeit Einblick in die Sicherheitslage Ihres Unternehmens und bekommen detailliert Auskunft über Schwachstellen. Mit DriveLock ist das Vulnerability Management eine einfache tägliche Routine. Schwachstellen-Dashboards liefern Details, die nach Schweregrad oder Art, Alter und betroffenen Endpunkten kategorisiert sind. Sie liefern die möglichen Schweregrade und Einstufungen sowie eine Beschreibung der aktuellen Schwachstellen und deren Behebung.

Diese Berichte stehen zur Verfügung:

Zustand der Verwundbarkeit der Systemumgebung

- Verteilung der Schwachstellenbewertungen
- Detaillierte Informationen über einen einzelnen Computer
- Entdeckte Schwachstellen, Scan-Datum und Status
- Informationen über erkannte Schwachstellen und Schwachstellen
- Scan-Abdeckung

Erkannte CVEs mit CVSS-Scores

- Base/Exploitability/Impact metrics

Konfiguration der Berichterstattung

- Unterdrücken von CVEs, die aus Gründen nicht gepatcht werden können oder sollen
- CVEs auf einzelnen Computern unterdrücken Entdeckte Schwachstellen, Scan-Datum und Status

Compliance-Berichte

- Vulnerability Management-Überblick
- Zustandsänderungen im Zeitverlauf
- Entwicklung der Verwundbarkeit und Bedrohungslage im Zeitverlauf

Schwachstellen-Statistik – Gesamtzahl an Schwachstellen

Zeigt die Gesamtzahl der Schwachstellen auf allen Geräten im Netzwerk an und klassifiziert den Schweregrad der Schwachstellen im Bereich Schwachstellen-Statistik als niedrig, mittel, hoch und kritisch.

Schwachstellen auf CVSS-Basis

Eine Priorisierung der Abhilfemaßnahmen kann nur dann erfolgen, wenn Einsicht in die Kategorie der Schwachstelle ermöglicht wird. DriveLock verwendet das Common Vulnerability Scoring System (CVSS), das den Schweregrad der Schwachstelle auf der Grundlage von Hauptmerkmalen bestimmt, die in eine numerische Bewertung übersetzt werden.

Kürzlich entdeckte Schwachstellen

Dies zeigt Schwachstellen auf, die erst kürzlich entdeckt wurden. Zeigt alle kürzlich bekannt gewordenen, aber noch nicht entdeckten Schwachstellen oder CVEs an irgendeinem Endpunkt.

Alter der Schwachstellen

Diese zeigt Schwachstellen, gruppiert nach der Anzahl der Tage, seit sie entdeckt wurden, und die noch nicht behoben wurden.

Top Schwachstellen

Diese zeigt die am stärksten gefährdeten Assets anhand ihrer CVE-ID und der Anzahl der gefährdeten Geräte.

Gefährdete Assets

Bestimmt die am stärksten gefährdeten Endgeräte und Software-Assets. Dies zeigt die auf den Systemen in der Organisation installierten Software-Assets und das damit verbundene Risiko entsprechend dem Grad ihrer Verwundbarkeit an. Klicken Sie auf einen Asset-Namen, um die Details des betroffenen Endpunkts anzuzeigen.

Anfällige Endpunkte

Zeigt die Gesamtzahl der Schwachstellen, die ein Host hat, und die Einstufung des Schweregrades, nach der sie gruppiert sind.

Trend der Verwundbarkeit und Bedrohungslevel im Zeitverlauf

Zeigt die zeitliche Abfolge von Schwachstellen an Endpunkten und deren Schweregrad. Administratoren können sehen, ob sie sich in die richtige Richtung bewegen.

von Andreas Fuchs, Director Product Management 2020-07

Kontaktieren Sie uns!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com