03 | 22 Sonderdruck für DataLocker

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

DataLocker SafeConsole mit Sentry K350

www.it-administrator.de

Quelle: Christian Knermann/dataLocker

DataLocker SafeConsole mit Sentry K350

In geheimer Mission

von Dr. Christian Knermann

DataLocker widmet sich mit der SafeConsole der zentralen Konfiguration und dem erhöhten Schutz von Wechseldatenträgern sowie virtuellen Laufwerken. IT-Administrator hat das System in der Praxis erprobt und war begeistert – besonders vom Zusammenspiel der Managementkonsole mit den speziell dafür konzipierten Datenträgern.

James Bond fände vermutlich gefallen an der Produktpalette von DataLocker. Doch auch abseits von Agentenromanen haben Unternehmen und Endanwender das berechtigte Interesse, Daten auf physischen Wechseldatenträgern sowie in Cloudspeichern zu verschlüsseln und vor dem Zugriff Dritter zu schützen. Hier positioniert sich der Hersteller mit Produkten rund um Storage-Hardware mit integrierter Verschlüsselung und der sicheren Ablage von Daten in Clouddiensten.

Vier Module zentral verwaltet

Die webbasierte SafeConsole bildet die Schaltzentrale für die vier einzeln oder in Kombination verwendbaren Module:

- Device Control dient der zentralen Konfiguration spezieller Wechseldatenträger mit integrierter Verschlüsselung. Solche als "SafeConsoleReady" zertifizierten USB-Festplatten und -Sticks bieten neben DataLocker selbst etwa auch noch die Hersteller Kingston und Origin Storage an.
- Anti-Malware als Ergänzung zur Device Control aktiviert eine in die SafeConsoleReady-Datenträger integrierte Abwehr von Schadsoftware auf Basis der Scan-Engine von McAfee. Der Datenträger selbst kann so Dateien untersuchen und im Fall erkannter Bedrohungen in Quarantäne verschieben – unabhängig davon, ob auf dem Windows-Computer, mit dem der Datenträger verbunden ist, eine Antimalware-Software aktiv ist.
- PortBlocker als Clientsoftware für Windows und macOS sperrt die USB-Ports eines Computers und lässt nur zentral vom Admin freigegebene Speichermedien zu, was unabhängig von oder in Kombination mit SafeConsoleReady-Datenträgern funktioniert.
- SafeCrypt, ebenfalls als Clientsoftware für Windows und macOS verfügbar, erzeugt und verwaltet virtuelle verschlüsselte Laufwerke, die entweder lokal oder in Clouddiensten, wie etwa Dropbox, Google Drive oder Microsoft OneDrive, liegen dürfen.

Management on-premises oder als Clouddienst

DataLocker bietet die SafeConsole in zwei Varianten an, wahlweise lokal zur Installation auf einem dedizierten Windows-Server im eigenen Rechenzentrum oder als SafeConsole Cloud (SCC). Letztere betreibt DataLocker als Single-Tenant-Host, also auf Basis eines einzelnen virtuellen Servers pro Kunden, für europäische Nutzer in den Rechenzentren von AWS in Irland. Sowohl die On-Premises-Variante als auch die Bereitstellung in der Cloud vertreibt DataLocker über Reseller in Form von jährlichen Mietlizenzen. Den einfachsten Einstieg bildet jeweils ein sogenanntes Standard Starter Pack. Hier darf der Kunde insgesamt 20 Lizenzen seiner Wahl aus den vier Modulen DeviceControl, PortBlocker, Anti-Malware und SafeCrypt kombinieren.

Anspruchsvollen Kunden bietet DataLocker gegen Aufpreis zusätzlich einen "Professional Plan". Der umfasst Premium-Support mit kurzen Reaktions- und Problemlösungszeiten, den Austausch de-

fekter Hardware über eine Rücksendeverwaltung sowie innerhalb der Konsole zusätzlich die Funktion ZoneBuilder. Damit definieren Admins anhand von IP-Adresskreisen und Clientzertifikaten Gruppen vertrauenswürdiger Endgeräte. Richtlinien legen dann etwa fest, dass SafeConsoleReady-Datenträger an diesen Endgeräten ihren Inhalt automatisch freigeben oder gar ausschließlich an den vertrauenswürdigen Endpunkten funktionieren. Der Enterprise Plan erweitert den Umfang der Variante Professional um die Integration mit SSO- und SIEM-Systemen sowie eine REST-API.

Robuste Hardware

Für unseren Test hatte uns DataLocker einen befristeten Zugang zur SCC mit allen vier Modulen sowie ein Exemplar des Wechseldatenträgers DataLocker Sentry K350 zur Verfügung gestellt. Dieser ist in Größen von 16, 64 und 256 GByte erhältlich. Es handelt sich um ein microSSD-Laufwerk im Format eines etwas größeren USB-Sticks – 100 mm lang, 20 mm breit und 11 mm dick bei einem Gewicht von 35 g. Das Gehäuse ist größtenteils aus Leichtmetall mit einigen Kunststoffelementen gefertigt.

Der Speicher macht einen hochwertigen Eindruck und genügt dem US-amerikanischen Militärstandard MIL-STD-810G sowie der Norm IP67, ist also unempfindlich gegen Staub und Untertauchen bis zu einer Wassertiefe von einem Meter. Weiterhin hat das US-amerikanische National Institute of Standards and Technology den Sentry K350 nach dem Standard FIPS 140-2 Level 3 zertifiziert. Der bescheinigt dem Gerät unter anderem, dass es über ein Rollenkonzept für den Zugriff verfügt und derart versiegelt ist, dass es sein Innenleben nicht zerstörungsfrei preisgibt.

Der Sentry K350 kümmert sich automatisch um den Schutz der darauf gespeicherten Daten. Der Stick setzt dazu auf AES-XTS-Blockverschlüsselung bei einer Schlüssellänge von 256 Bit. Das Gerät ist komplett autark und ohne Anbindung an die SCC verwendbar. Es verfügt dazu über ein kleines OLED-Display sowie eine Tastatur mit zwölf Tasten (Bild 1), die haptisches Feedback geben und so die Konfiguration und Eingabe von alphanumerischen Passwörtern erlauben. Buchstaben und Sonderzeichen erreichten wir durch mehrfaches Drücken der einzelnen Tasten, wie von Mobiltelefonen aus der Vor-Smartphone-Ära bekannt.

Mit dem richtigen Passwort entsperrt, gibt der Stick seinen Inhalt per USB-A-Stecker nach dem Standard USB 3.2 Gen 1 frei. Das Gerät verhält sich gegenüber einem Computer wie herkömmliche USB-Massenspeicher, benötigt also keine speziellen Treiber und funktioniert damit unabhängig vom Betriebssystem des Clients. Der Sentry K350 besitzt einen integrierten Lithium-Ionen-Akku zur Versorgung des Displays. Bei leerem Akku empfiehlt der Hersteller, das Gerät vor Verwendung zunächst für 30 Minuten per USB-Schnittstelle aufzuladen. Es funktioniert aber grundsätzlich auch bei leerem oder gar defektem Akku mit externer Spannungsversorgung per USB.

Bild 1: Mit dem Sentry K350 hat DataLocker einen IP67-geschützten Speicher mit Hardwareverschlüsselung im Angebot.

Zugriff nur mit Passwort

Sobald wir den K350 aufgeladen und eingeschaltet hatten, forderte das Gerät uns auf, ein Admin-Passwort von mindestens acht Zeichen Länge zu setzen. Grundsätzlich darf ein Passwort auch nur aus Ziffern bestehen, doch allzu simple Folgen wie etwa 12345678, 78901234, 43210987 oder 1111111 akzeptierte der Stick nicht.

Anschließend verlangte der Stick bei jedem Einschalten nach unserem Passwort. Daraufhin konnten wir mittels der beiden Pfeiltasten durch das Hauptmenü des OLED-Displays navigieren. Die erste Option "Connect" gibt den Speicher für Schreibzugriffe frei. Wir konnten den Stick somit wie jeden anderen Massenspeicher an beliebigen Computern anschließen und

DataLocker SafeConsole mit Sentry K350

Produkt
Zentrale Verwaltung von USB-Ports und Wechseldatenträgern mit Hardwareverschlüsselung.

Hersteller
DataLocker
https://datalocker.com

Preis
Der USB-Speicher Sentry K350 kostet mit 16 GByte Speicherkapazität 175 Euro, mit 64 GByte etwa 240 Euro und mit 256 GByte rund 420 Euro. Die SafeConsole ist im Standard Starter Pack (umfasst 20 Lizenzen frei wählbar aus den Modulen DeviceControl, PortBlocker, Anti-Malware und SafeCrypt) in der Cloudvariante für rund 1000 Euro pro Jahr und in der On-Premises-Version für etwa 1800 Euro im Jahr erhältlich.

Dazu kommen 24 Euro pro Jahr für jede weitere DeviceControl-Lizenz und 14 Euro im Jahr pro weitere PortBlocker-Lizenz. Dreijahreslizenzen sind ebenfalls erhältlich und reduzieren den Preis pro Jahr um ungefähr 16 Prozent.

Systemvoraussetzungen
Im Standalone-Betrieb reicht für den Sentry K350 ein Clientcomputer mit USB-A-Port. Für die SafeCloud-Anbindung des Sticks ist ein Rechner mit Windows nötig. PortBlocker und SafeCrypt funktionieren mit Windows und macOS. Unter dem Apple-Betriebssystem läuft PortBlocker aber nur auf Intel-Macs.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

verwenden. Die zweite Option "Read-only" ist selbsterklärend. Der "Boot mode" unterstützt die Installation eines Betriebssystems, ist aber nur verfügbar, wenn der K350 nicht in die zentrale Verwaltung der SafeConsole eingebunden ist.

Im schlicht "Menu" betitelten Konfigurationsbereich konnten wir einige grundlegenden Einstellungen vornehmen. So durften wir hier eine zusätzliche User-Rolle aktivieren. In diesem Fall bietet der Stick beim nächsten Start die beiden Rollen "Admin" und "User" zur Auswahl an. Letztere muss ein separates Passwort setzen. Beide Rollen haben gleichermaßen Zugriff auf den Speicher des Mediums, doch der User hat nur eingeschränkte Möglichkeiten der Konfiguration. Der größte Vorteil der Rollen: Sollte der Anwender sein Passwort vergessen, kann der Admin ihm helfen.

Integrierter Selbstzerstörungsmodus

Unter dem Menüpunkt "Self Destruct" konnten wir in einem Bereich von mindestens 10 bis maximal 50 festlegen, nach wie vielen falschen Passworteingaben das Gerät sich selbst zerstören soll. Und dies ist tatsächlich wörtlich zu verstehen. Das standardmäßig ausgewählte Verfahren "Destroy data" löscht zwar nur Konfiguration sowie Inhalt des K350 und der Stick ist danach jungfräulich und lässt sich neu konfigurieren. Doch die zweite Option namens "Destroy device" macht die Hardware tatsächlich irreversibel unbrauchbar.

Um den Stick zurückzusetzen, mussten wir nicht zehn Mal ein falsches Passwort eingeben. Der Menüpunkt "Zeroize drive" löscht ebenfalls Konfiguration und Inhalt des Geräts. Zuvor fragte uns der K350 dreimal, ob dies wirklich unsere Absicht ist.

Noch schneller geht es über den etwas versteckten "SilentKill Code", den nur der Admin konfigurieren darf. Hierzu mussten wir beim Ändern des Passworts die Enter-Taste länger als fünf Sekunden gedrückt halten. Anschließend konnten wir den Kill-Code festlegen. Der K350 warnt unmissverständlich davor, was es mit diesem zusätzlichen Passwort auf sich hat: Wer beim Entsperren des Sticks den Code statt seines Passworts eingibt, löst ohne weitere Rückfrage sofort das im Bereich "Self Destruct" konfigurierte Löschverfahren aus – James Bond lässt hier grüßen.

Weiterhin konnten wir in der Konfiguration komplexere Passwörter aktivieren, die neben Ziffern mindestens auch einen Buchstaben und ein Sonderzeichen enthalten müssen, und zudem die Mindestlänge der Passwörter von 8 auf 64 Zeichen erhöhen. Einmal aktiviert, sperrt die "Auto-Lock Time" das Gerät automatisch nach einer Zeit der Inaktivität im Bereich von 10 bis 720 Minuten. Der "Read-Only Mode" lässt sich vom User nicht deaktivieren und erzwingt, dass sich das Gerät nur noch schreibgeschützt entsperrt.

Der Sentry K350 bietet somit bereits bei alleinstehender Verwendung flexible Konfigurationsoptionen. Doch erst die SafeConsole verwaltet eine größere Flotte von Datenträgern komfortabel.

Zentrale Verwaltung über Policies

Dazu meldeten wir uns unter "https://<Kundenname>.safeconsolecloud.com" an der SCC an, die zunächst nach Bestätigung der Lizenzbedingungen verlangte und uns anschließend die Release-Notes der zum Testzeitpunkt aktuellen Version 5.9 präsentierte. Das Dashboard gibt einen Überblick über sämtliche zu verwaltende Endpunkte und Benutzer, die wir dann im Bereich "Manage" unterteilt in die vier Kategorien "Policies", "Users", "Drives" und "PortBlocker" im Detail konfigurieren konnten (Bild 2). Benutzer legten wir wahlweise manuell oder per CSV-Import an. Die SCC kann sowohl mit lokalen Benutzerkonten als auch mit solchen in einer Active-Directory-Domäne umgehen.

Das Herzstück der Verwaltung bilden die Policies, die sämtliche Einstellungen für Benutzer, Clientrechner sowie physische und virtuelle Datenträger zentral steuern. Die Konsole wies uns darauf hin, dass die Default Policy noch nicht konfiguriert sei und leitete uns in den zugehörigen Verwaltungsbereich.

Abweichend davon konnten wir später angepasste Richtlinien für Gruppen von Benutzern, Laufwerke sowie Clientcomputer mit installiertem PortBlocker definieren. Doch zunächst beließen wir es bei einer Standardrichtlinie. Jede Richtlinie unterteilt die Konfiguration zuoberst in mehrere Register für die DataLocker-Software der Versionszweige 6.x und 4.8.x sowie spezifische Einstellungen für verschiedene Hardware, darunter unser Sentry K350 sowie SafeCrypt- und PortBlocker-Clients.

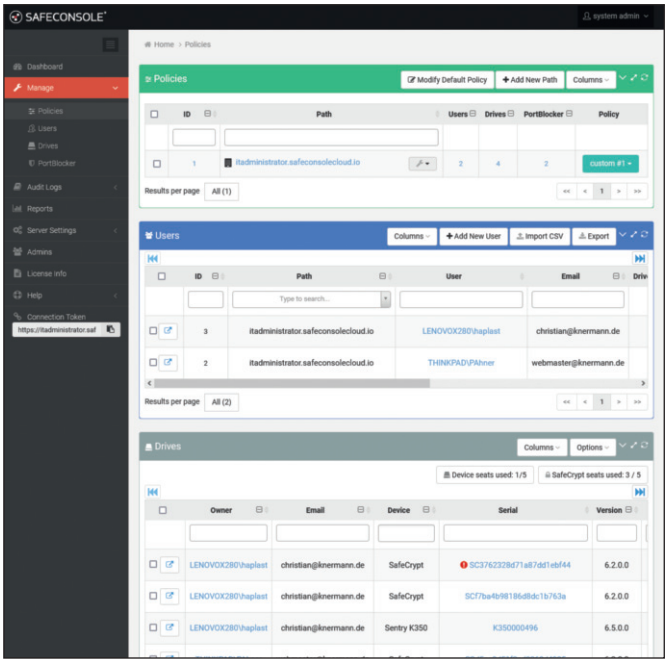

Bild 2: Die SafeConsole verwaltet Richtlinien, Benutzer, Laufwerke und PortBlocker-Clients.

Hier nahmen wir nun Einstellungen für den K350 vor, etwa zentral die Komplexität der Passwörter oder die Auto-Lock-Zeit. Die Konfiguration des Selbstzerstörungsmodus findet sich ebenfalls im Bereich der "Password Policy". Die Konsole bezeichnet diese als "Bruteforce Action" für den Fall, dass der Stick die definierte Anzahl an falschen Passworteingaben erreicht. Zur Wahl standen hier "Factory Reset" oder die plakativ als "Detonate" bezeichnete Ak-

tion, wiederum verbunden mit dem Warnhinweis, dass diese den K350 dauerhaft unbrauchbar macht. In den Eigenschaften des Sticks konnten wir diese Aktionen auch unmittelbar veranlassen (Bild 3).

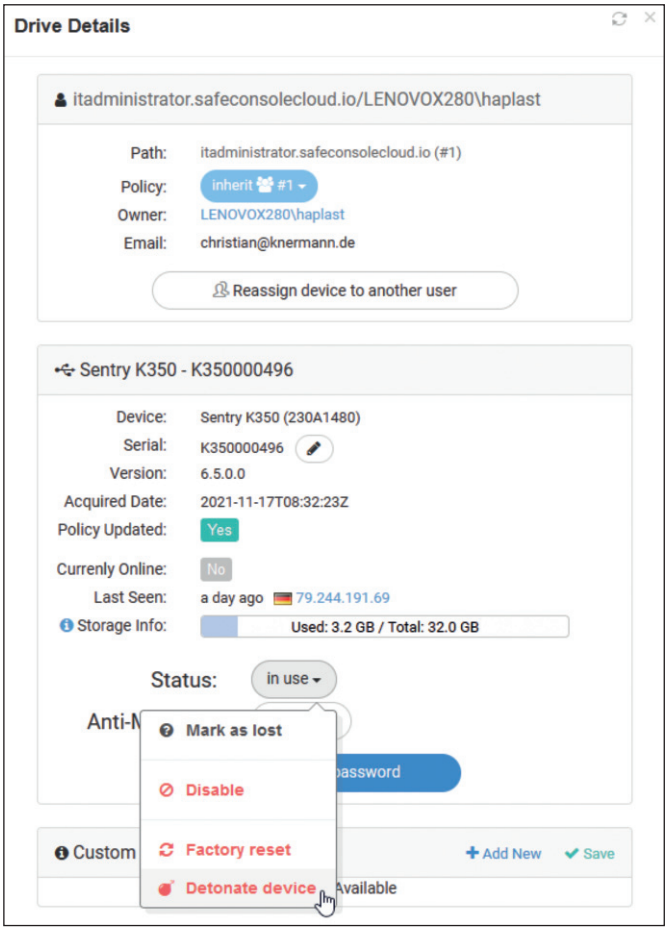

Bild 3: Die SafeConsole setzt kompatible Geräte aus der Ferne zurück oder macht sie komplett unbrauchbar.

Sentry K350 mit erweiterten Optionen

Die weiteren Optionen gehen deutlich über die Funktionalität eines alleinstehenden Sticks hinaus. So konnten wir den K350 mittels einer Einschluss- oder Ausschlussliste anweisen, bestimmte Dateitypen, etwa ausführbare Dateien, nicht zu akzeptieren oder nur genau die aufgeführten Dateiendungen zuzulassen. Wir konnten die integrierte Antimalware-Engine von McAfee aktivieren und diese sogar derart restriktiv einstellen, dass der Stick seinen Speicher erst freigibt, sobald er die Antivirus-Pattern aktualisiert und seinen Inhalt gescannt hat.

Die Audits protokollieren auf Wunsch sämtliche Aktivitäten bis hin zu einzelnen Dateioperationen. ZoneBuilder und Geofence schränken die Verwendung optional auf bestimmte Clients, IP-Adresskreise und geografische Regionen ein. Die SCC erzeugt dazu wahlweise selbstsignierte Zertifikate oder verwendet solche einer bereits im Unternehmen vorhandenen CA. Speziell für den K350 konnten wir noch die sogenannten Stand-alone-Logins aktivieren und eine maximale Anzahl solcher Logins festlegen, doch dazu gleich mehr.

SafeConsole aktuell nur mit Windows

Um die Policies in Kraft zu setzen, verknüpften wir nun den K350 mit der SCC. Dazu hatten wir den Stick zurückgesetzt, neu initialisiert und über das OLED-Display in der Konfiguration den Punkt "Menu / SafeConsole" aktiviert. Damit änderte sich das Verhalten des Geräts. Sobald wir dieses entsperrten und mit einem Computer verbanden, erschien im OLED-Display der Hinweis "Launch Unlocker" und im Datei-Explorer fanden wir zunächst nur eine "Unlocker" genannte, 42 MByte große Partition mit der Datei "Unlocker.exe" darauf vor. Der Unlocker-Client funktioniert aktuell nur unter Windows. DataLocker möchte perspektivisch zwar auch macOS unterstützen, bis zum Redaktionsschluss war aber leider noch kein konkreter Zeitplan hierfür bekannt. So beschränkten wir uns auf Windows 10 21H2 sowie Windows 11, wo die weiteren Schritte jeweils ohne Probleme funktionierten.

Der Unlocker führte uns durch die Registrierung. Dazu mussten wir zunächst einen Token eintragen. Diese URL der Form "https://<Kundenname>.safeconsolecloud.io/connect" fanden wir online in der Konsole. Anschließend registrierten wir den K350 mittels eines individuellen Nutzer-Tokens, das wir ebenfalls der Konsole entnehmen konnten. Nachdem wir unsere E-Mail-Adresse bestätigt hatten, wählten wir das gewünschte Format der sicheren Datenpartition (FAT32, exFAT oder NTFS), woraufhin auch die zweite Partition für die Daten mit einem separaten Laufwerksbuchstaben im Datei-Explorer erschien.

Von nun an lief jede Entsperrung zweistufig ab. Zunächst gaben wir lokal am K350 unser Passwort ein und verbanden diesen mit einem Windows-System. Dann starteten wir den Unlocker, der mit der SafeConsole Kontakt aufnahm und erst dann die sichere Datenpartition freigab. Das funktionierte auch in Verbindung mit der integrierten Antimalware-Abwehr, wovon wir uns anhand der bekannten EICAR-Antivirus-Testdatei überzeugten. Das Testvirus landete umgehend in der Quarantäne. Im Fall eines vergessenen Passworts erzeugten wir in der SCC einen Reset-Code, den wir dem betroffenen User telefonisch oder direkt aus der Konsole heraus per E-Mail übermitteln konnten.

Der mit der SafeConsole verzahnte K350 funktioniert für eine begrenzte Anzahl von Einsätzen jedoch auch offline oder mit einem anderen Betriebssystem, wie macOS, Chrome OS oder Linux. Hier hilft der Standalone-Modus, den wir zentral per Policy aktivierten. Nachdem unser Stick die Richtlinie aktualisiert hatte, konnten wir in der Rolle eines Nutzers über den Unlocker den Standalone-Modus anfordern. Dabei mussten wir einen Grund für diese Anforderung angeben. Zur Auswahl standen dafür Bequemlichkeit, plattformübergreifende Nutzung oder ein benutzerdefiniertes Freitextfeld.

Anschließend konnten wir bei der nächsten Verwendung nach Eingabe des Passworts im Display des K350 wählen, ob wir diesen in Verbindung mit der SafeConsole oder allein nutzen wollten. In letzterem Fall gab der Stick ohne Umweg über den Unlocker direkt die sichere Datenpartition frei und zählte die Anzahl maximal möglicher Stand-alone-Anmeldungen herunter. Sobald wir alle Anmel-

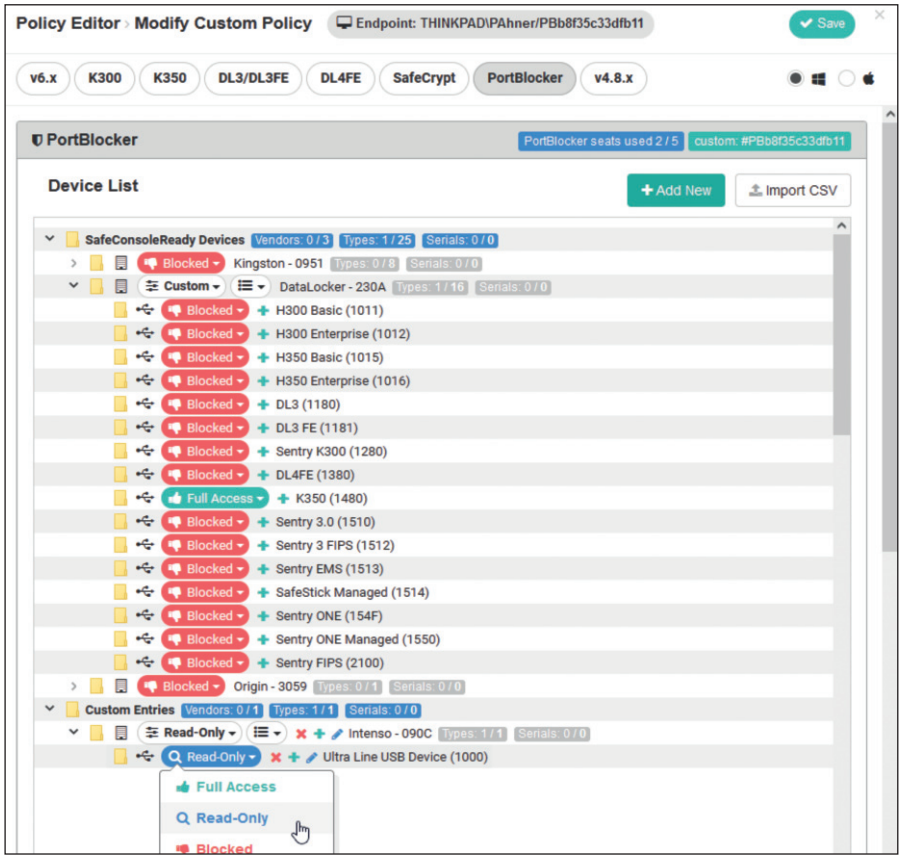

Bild 4: PortBlocker erlaubt oder blockiert USB-Massenspeicher anhand ihrer Vendor- und Product-IDs.

dungen verbraucht hatten, musste das Gerät zwingend wieder an einem Windows-Client Kontakt zur SCC aufnehmen.

USB-Massenspeicher schnell blockiert

Mittels PortBlocker konnten wir die Sicherheit weiter erhöhen, indem wir die USB-Ports der Clients beschränkten. Das funktioniert aktuell für Windows sowie macOS, in letzterem Fall allerdings nur für Macs mit Intel-Prozessor. Unterstützung für die ARM-basierten Apple-M1-Prozessoren plant DataLocker zwar, konnte jedoch noch keinen Zeithorizont hierfür benennen.

Nach der Installation des PortBlocker-Clients, den wir im Lizenzbereich der SafeConsole fanden, mussten wir diesen analog zum Unlocker des K350 an der Konsole registrieren. Darauf sperrte PortBlocker zunächst die USB-Ports unseres Clients für sämtliche Massenspeicher. Über die Policies konnten wir dann gezielt bestimmte Geräte wieder zulassen. Dazu bringt die SCC vorgefertigte Einträge für alle SafeConsoleReady-Geräte mit. Eigene Geräte konnten wir anhand ihrer USB-Vendor-ID (VID) und -Product-ID (PID) selbst in der Policy hinterlegen. VID und PID unserer sonstigen USB-Massenspeicher ermittelten wir dazu unter Windows mittels des kostenlosen Tools NirSoft USBDeview. Je nach individuellem Schutzbedarf sorgt eine Policy so dafür, dass PortBlocker etwa ausschließlich SafeConsoleReady-Speicher für schreibenden Zugriff freigibt und anderweitige Geräte entweder lesend einbindet oder ganz blockiert (Bild 4).

Sicher speichern in der Cloud

Das vierte Modul SafeCrypt half uns dabei, virtuelle Laufwerke zu erzeugen. Dies funktionierte ähnlich den anderen Modulen. Der SafeCrypt-Client läuft sowohl unter Windows als auch unter macOS, in diesem Fall sogar problemlos mit dem M1-Prozessor, wovon wir uns an unserem Testclient mit macOS 12 Monterey überzeugen konnten. So gaben wir auch hier den Token zur SCC ein und konnten im Client verschlüsselte Ordner anlegen, die wir wiederum über individuelle Token pro User in der SCC registrierten.

Ein solcher Ordner kann gefahrlos in einer Public Cloud liegen. Er gibt seinen Inhalt nur preis, wenn er per SafeCrypt-Client mit dem richtigen Passwort entsperrt wird. Das Kennwort konnten wir ändern oder mittels "Action / Password help" zentrale Unterstützung bei vergessenen Credentials anfordern.

Dazu mussten wir einen auf dem Client erzeugten String von acht Zeichen Länge an den Admin übermitteln, der mit dieser Information innerhalb der SCC einen Entsperrcode erzeugte und an den User zurückübermittelte. Daraufhin konnten wir dann ein neues Passwort für den sicheren Speicher vergeben.

Fazit

Die DataLocker SafeConsole bietet mit der Kombination ihrer vier Module ein stimmiges Paket für die Absicherung von physischen und virtuellen Wechseldatenträgern. Der Sentry K350 ist bereits bei der alleinstehenden Verwendung ein praktischer Begleiter, nicht nur für angehende Geheimagenten. Sein ganzes Potenzial entfaltet der robuste und sichere USB-Speicher im Zusammenspiel mit der zentralen Verwaltung per SafeConsole. *(ln)* IT

So urteilt IT-Administrator

K350 als Standalone	8
K350 mit SCC-Integration	10
Antimalware	7
PortBlocker	8
SafeCrypt	8

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Unternehmen mit Windows-Clients und hohen Anforderungen an die Sicherheit von Wechseldatenträgern.

bedingt für Firmen mit Clients unter Apple macOS oder Linux.

nicht für Organisationen ohne besonderen Schutzbedarf für den Zugriff auf Wechseldatenträger.