N-ABLE™

# N-central Geräterollback in N-able EDR:

## Ihre Zeitmaschine für mehr Cybersicherheit

## E-Book

# Geräterollback in N-able EDR: Ihre Zeitmaschine für mehr Cybersicherheit

EDR erfasst ein breiteres Spektrum an Bedrohungen, leistet in puncto Erkennung und Datensicherheit also mehr als ein normaler Virenschutz, der nur dateibasierte Malware auf der Grundlage von Virensignaturen erkennen kann. EDR-Lösungen sind außerdem zu maschinellem Lernen fähig und analysieren das Verhalten von Endpunkten. Dadurch bieten sie mehr Schutz vor Zero-Day-Angriffen. Kurz gesagt: Für Unternehmen, die große Bestände sensibler Daten verarbeiten, ist EDR das Mittel der Wahl.

Vorbeugen ist besser als heilen, wie jeder weiß. Doch manchmal bedarf es eben einer Heilung, und diese kann dank EDR-Software, beispielsweise N-able™ Endpoint Detection and Response, wesentlich schneller und besser erfolgen. Insbesondere die Möglichkeit zu Rollbacks, wie sie N-able EDR bietet, erspart Ihnen viel Zeit bei der Vorfallsbehandlung – und Ihren Kunden kostspielige Systemausfälle. Der Rollback ist einer der ganz wesentlichen Unterschiede zwischen EDR und AV. Doch der Reihe nach. Wir erklären Ihnen, wie N-able EDR mit erkannten Bedrohungen umgehen kann, bevor ein Rollback veranlasst wird.

## Eine Kette von Optionen

Eine gute EDR-Lösung zeichnet sich dadurch aus, dass sie den Großteil ihrer Vorfallsreaktionen automatisiert. Ohne EDR müssen Sie vieles davon manuell tun. Wenn N-able EDR eine Bedrohung als solche markiert hat, bietet es für den Umgang damit fünf verschiedene Optionen. Drei davon sind präventiv, gebieten der Malware also Einhalt, bevor sie Schaden anrichtet. Die anderen beiden sind reaktiv; sie versetzen betroffene Endpunkte wieder in einen einwandfreien Zustand.

Sehen wir uns die Optionen nacheinander an.

### PRÄVENTION

- **Löschung:** Diese Option erstickt einen Angriff im Keim, beispielsweise einen bösartigen Prozess, der auf Ihrem Computer im Hintergrund ausgeführt wird. Hat die EDR ihn erkannt, beendet sie ihn sofort. Oder ein Excel®-Dokument möchte ein Skript starten, das massenhaft Dateien löschen soll. Die EDR verhindert die Ausführung dieses Skripts. Ohne EDR müssten Sie derlei Vorgänge selbst abfangen und auf manuellem Wege stoppen.
- **Quarantäne:** Die Quarantänefunktion verschiebt die ausführbaren Malwaredateien in einen abgeschirmten Bereich, aus dem heraus sie keinen weiteren Schaden anrichten können. In einer Sandbox-Umgebung können solche Dateien dann eingehender untersucht werden. Eine Quarantänefunktion gibt es auch in herkömmlichen AV-Lösungen.
- **Trennung vom Netzwerk:** Mit dieser Option können Sie einen infizierten Endpunkt vom Netzwerk nehmen, was Administratoren den Umgang mit der Malware erleichtert. Der ausgehende Netzwerkdatenverkehr wird dabei auf die Managementkonsole beschränkt. So kann sich die Malware von dem Gerät aus nicht weiter im Netzwerk verbreiten. Kriminelle versuchen, aus jedem ihrer Angriffe das Optimum herauszuholen. Einmal eingeschleuste Malware soll sich auf möglichst viele Geräte im Netzwerk verteilen, um möglichst viele Daten stehlen zu können. Die Trennung

eines befallenen Endpunkts vom Netzwerk unterbricht die Infektionskette an dieser Stelle. Anschließend können Sie mit den ausgefeilten forensischen Tools von EDR genauer untersuchen, was geschehen ist. So gewinnen Sie Zeit für den Umgang mit kniffligen Problemen, für die es keine schnelle Standardlösung gibt. Sie verstehen so auch besser, was vorgefallen ist. Dies ist wichtig für die künftige Prävention (und um sicherzustellen, dass keine anderen Systeme befallen sind). Kurz gesagt: Geräte vom Netzwerk zu trennen, bietet mehrere Vorteile.

### REAKTION

- **Fehlerbehebung:** Mit dieser Funktion können Sie durch einen Angriff verursachte Schäden reparieren. Fehlerbehebung bedeutet allerdings nicht Rollback – Letzterer versetzt das Gerät in einen ganz bestimmten Zustand zurück.
- **Rollback:** Bei einem Rollback wird das betroffene Gerät auf eine so genannte VSS-Kopie (Volume Shadow Copy Service) zurückgesetzt, um den Schaden zu beheben. Es soll mit anderen Worten ein Zustand wiederhergestellt werden, den das Gerät vor seiner Infektion hatte. Das ist besonders bei Ransomware-Angriffen hilfreich. Wer auf unverschlüsselte Versionen seiner Gerätedateien zurückgreifen kann, ist nicht mehr durch Kriminelle erpressbar. Weiteres Plus: Der Rollback erfolgt mehr oder minder sofort, geht also viel schneller als die Wiederherstellung per Backup. Dennoch ist EDR kein Ersatz für eine zuverlässige cloudbasierte Backup-Lösung, schließlich ist Ransomware nur eine von vielen Gefahren. Auch Softwarefehler, Hardwareprobleme oder Naturkatastrophen können zu Datenverlusten führen. Außerdem ist die Rollbackfunktion nur für Windows® verfügbar. Für Geräte mit macOS® und Linux® sind solide Cloud-Backups also unumgänglich.

Die EDR greift nacheinander auf alle fünf Glieder der Optionenkette zurück. Sie können die EDR als Administrator zwar zu dezidierten Handlungen anweisen, zum Beispiel als prioritär auszuführende Aktion „Quarantäne“ festlegen. Trotzdem wird die EDR alle jeweils vorgelagerten Optionen (im Fall der Quarantäne also „Löschen“) ausführen.

## Rollback: technische Voraussetzungen

Das Potenzial des automatischen Rollbacks ist enorm, denn mit seiner Hilfe können Sie ein Kundensystem im Handumdrehen wiederherstellen und Ihren Kunden unangenehme Situationen (etwa durch Ransomware) ersparen.

Hinter dem Rollback steht eine Technik namens VSS. Die in Microsoft® Windows verfügbare Funktion fertigt Kopien von ganzen Volumes oder Computerdateien an, und zwar auch dann, wenn diese gerade in Verwendung sind.

VSS ist im Grunde etwas Ähnliches wie Digitalfotografie: Jedes Bild erhält einen Datums- und Zeitstempel. In bestimmten Abständen wird eine digitale Momentaufnahme des Systems gespeichert, die dann im Infektionsfall zur Überschreibung des Geräts genutzt werden kann. Dank VSS hat der Benutzer ein Bild seines Systems vor dem Angriff zur Verfügung. Eine höchst praktische Funktion und besonders wirksam durch die Möglichkeit zum Rollback.

Bei alledem ist der Ressourcenverbrauch durch VSS geringer, als man denken würde. Die Technik arbeitet inkrementell, verschiebt also immer nur diejenigen Dateien an einen temporären Ablageort, die sich seit dem letzten Schnappschuss verändert haben. Das geht natürlich wesentlich schneller, als jedes Mal eine Aufnahme des kompletten Systems zu machen.

VSS wurde mit den Betriebssystemen Windows XP® und Server 2003 eingeführt und ist seitdem fester Bestandteil von Windows. Die Rollbackfunktion von N-able EDR ist in Agenten ab Windows Vista® und Windows Server® 2008 R2 aufwärts verfügbar. Achtung: Ein Rollback per VSS von Geräten mit macOS® oder Linux ist derzeit nicht möglich.

## Was bringt der Rollback?

Warum ist es so wichtig, die Möglichkeit zum Rollback zu haben? Weil der Ernstfall allzu schnell eintreten kann: Ein Klick auf einen betrügerischen Anhang oder Link in einer E-Mail genügt, damit Ransomware ein Netzwerk befallen, Dateien verschlüsseln, Computer sperren und so den gesamten Betrieb lahmlegen kann.

**Ransomware ist alles andere als harmlos:**

- Ende 2019 verzeichneten Unternehmen im Schnitt 16,2 Tage Ausfallzeit aufgrund von Ransomware.[1]
- Experten zufolge wird im Jahr 2021 alle 11 Sekunden ein Unternehmen Opfer eines Ransomware-Angriffs werden.[2]
- Die Schäden durch Ransomware werden 2021 weltweit voraussichtlich 20 Milliarden US-Dollar kosten.[3]

Ransomware-Angriffe können Unternehmen in ein finanzielles Desaster stürzen. Je schneller Sie Ransomware erkennen, desto besser können Sie ihre Verbreitung stoppen. Mit dem Rollback bereits befallener Geräte können Sie Kunden vor Systemausfällen und deren Folgekosten bewahren. Die Wiederherstellung der Endpunkte lässt sich außerdem ohne große Störung der Benutzer durchführen – ein weiterer Aspekt, der die Rollbackfunktion attraktiv macht.

Zugegeben, EDR kostet pro Endgerät etwas mehr als reiner Virenschutz, allerdings bekommen Sie auch mehr dafür: bessere Erkennung, automatische Vorfallsreaktion und die Möglichkeit zum Rollback. Verglichen mit den Kosten, die ein Cyberangriff nach sich ziehen kann, rechtfertigt sich die Investition in EDR von ganz alleine.

Sowohl AV als auch EDR haben ihre Berechtigung und jeweils sinnvolle Einsatzzwecke, allerdings: Es dauert vier bis sechs Stunden, einen infizierten Endpunkt wiederherzustellen – ein Zeitaufwand, den Sie Ihren Technikern und Kunden durch EDR ersparen würden. Die Mehrkosten pro Lizenz wären sicher eine gute Investition, besonders dann, wenn Sie große Netzwerke mit vielen Endpunkten betreuen, da der Reparaturaufwand hier schnell unermesslich werden kann. Denken Sie außerdem an die hohen Kosten, die mit jedem Systemausfall verbunden sind. Können Mitarbeiter nicht arbeiten, senkt dies die Produktivität und den Gewinn des Unternehmens. Mit EDR können Sie dem vorbeugen.

## Rollback in Aktion

Hackerangriffe, insbesondere mit Ransomware, fügen Unternehmen großen Schaden zu und sorgen immer wieder für hohe Kosten. Der Kampf dagegen mag anstrengend sein, ist aber machbar. Mit N-able EDR können Sie nach einem Angriff Endpunkte im Nu auf einen unversehrten Zustand zurücksetzen und geben Ihren Kunden dadurch besseren Schutz und das Gefühl einer lückenlosen Sicherheit.

[1] „Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate“, Coveware. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate (aufgerufen September 2020).

[2] „Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021“, Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (aufgerufen September 2020).

[3] „Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021“, Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (aufgerufen September 2020).

# N-able N-central mit integrierter EDR

Mit N-able EDR, integriert in N-central®, haben Sie direkt in der Lösung, mit der Sie die gesamte IT-Infrastruktur überwachen und verwalten, Funktionen für die erweiterte Gefahrenerkennung, Endgeräteüberwachung und schnelle Fehlerbehebung. Von EDR abgesehen, bietet N-central u. a. auch AV-Schutz. Sie können also jedem Kunden und Benutzer mühelos die jeweils geeignete Schutztiefe anbieten.

Die vielen integrierten Automatisierungsfunktionen von N-able N-central, etwa der Drag-and-Drop-Editor für die Einrichtung vollautomatischer Abläufe ganz ohne Programmier- oder Skriptkenntnisse, unterstützen Sie dabei, Ihre Aufgaben effizient zu erledigen.

Erfahren Sie mehr über die Integration von N-able EDR in N-able N-central:

# Über N-able

Mit N-able können Managed Services Provider (MSPs) kleine und mittelständische Unternehmen effektiv bei der Digitalisierung unterstützen. Eine flexible Technologieplattform und leistungsstarke Integrationen erleichtern MSPs die Überwachung, Verwaltung und Sicherung der Systeme, Daten und Netzwerke ihrer Endkunden. Unser wachsendes Portfolio an Sicherheits-, Automatisierungs- sowie Backup- und Wiederherstellungslösungen richtet sich an Fachleute für das IT-Servicemanagement. N-able vereinfacht komplexe Umgebungen und sorgt dafür, dass Kunden ihre Probleme selbst in die Hand nehmen können. Wir bieten umfassenden, proaktiven Support in Form von hilfreichen Partnerprogrammen, praktischen Schulungen und wachstumsfördernden Ressourcen. So können MSPs hochwertige Services liefern und ihren Erfolg ausbauen.

**n-able.com/de**