MICRO FOCUS

Produktdatenblatt

ZENworks Endpoint Security Management
ZENworks Full Disk Encryption

ZENworks Endpoint Security Management und ZENworks Full Disk Encryption

Es ist Freitag, 6:00 Uhr morgens. Wissen Sie, wo sich Ihre Endgeräte befinden? Eines davon – ein Notebook – wird gerade gehackt. Der Benutzer sitzt in einem Internetcafé. Er surft im Netz und denkt, dass die als „Internetcafé“ gekennzeichnete Verbindung sicher ist. Doch neben ihm sitzt ein Hacker, der sich mithilfe dieser Webfassade direkten Zugriff auf Ihre Unternehmensdatenbank verschafft.

ZENworks Endpoint Security Management und ZENworks Full Disk Encryption im Überblick

- **Verschlüsselung:**
  Verschlüsselung von Daten auf mobilen Geräten
- **Dynamische Sicherheit:**
  Schutz mithilfe von benutzer- und standortabhängigen Sicherheitsstufen sowie angemessene Anpassung von Richtlinien
- **Produktivität und Sicherheit aufrechterhalten:**
  Bereitstellung aller Ressourcen, die Ihre Benutzer für eine produktive tägliche Arbeit benötigen, ohne Sicherheitslücken offen zu lassen
- **Einzeln oder als Teil dieser Software enthalten:**
  ZENworks Suite

Jemand hackt Ihr System und Ihrem Benutzer fällt nichts auf. Er denkt nicht, dass ihm das passieren könnte, da er sich sicher fühlt.

Doch der Hacker könnte jetzt ungestört vertrauliche Daten von Ihrem Unternehmens-Notebook entwenden.

Risikofaktor Endgerät

Endgeräte stellen in jedem Unternehmen ein Sicherheitsrisiko dar, denn mehr als 70 Prozent Ihrer wertvollsten Daten werden auf ihnen transportiert.

Hierbei geht es nicht nur darum, sich vor Dieben zu schützen, die mit Ihren Geräten davonlaufen (auch wenn diese natürlich auch gestoppt werden müssen). Mindestens ebenso wichtig ist es jedoch, Ihre Daten zu schützen, während sie von Ihren Mitarbeitern verwendet werden.

Neben den oben beschriebenen „Man-in-the-Middle“-Angriffen lauern zahlreiche weitere Gefahren, vor denen Sie Ihr Unternehmen schützen müssen. Dazu gehören:

- **Drive Bombing:** „Zufällig gefundene“ oder „kostenlos“ angebotene USB-Sticks dienen als Träger von Viren, die über die Autorun-Funktion unbemerkt in Ihr System eingeschleust werden.
- **Thumb Sucking:** Benutzer bringen ihre USB-Sticks mit zur Arbeit und ziehen Daten darauf. Dadurch geraten die Daten jedoch außer Kontrolle. Ihre Daten können dann nicht mehr durch Ihre Sicherheitsrichtlinien geschützt werden.
- **Diebstahl:** Jemand stiehlt ein Notebook. Noch schlimmer ist es, wenn Mitarbeiter und andere Insider Schwachstellen ausnutzen, um sich persönliche Vorteile zu verschaffen.
- **Hackerangriff:** Malware kann über Ihre Geräte an der Firewall vorbei in Ihr System eingeschleust werden und verursacht u. U. Schäden im gesamten Unternehmen.

Sie ergreifen Gegenmaßnahmen und legen Regeln und Richtlinien fest. Doch wie gewährleisten Sie ihre Durchsetzung? Sie können eine Verschlüsselung einführen, doch dies

Sie benötigen eine Möglichkeit zur Durchsetzung der Richtlinien, die Ihrem Unternehmen umfassenden Schutz bieten – denn blindes Vertrauen könnte schwerwiegende Folgen haben. Sie benötigen Novell ZENworks Endpoint Security Management, um für die kontinuierliche Durchsetzung von Richtlinien zu sorgen.

kann teuer werden. Und was passiert, wenn der Benutzer sein bzw. ihr Passwort verliert? Dann hat niemand Zugriff auf die Daten. Es muss also eine Lösung bereitgestellt werden.

Richtlinienbasierte Sicherheit

Leider stellt der Faktor Mensch immer noch die größte Gefahr dar. Die Bedrohung durch Hacker ist allgegenwärtig, aber auch Insider können Ihrem Unternehmen schaden. Viele sind mit sicherem Computing einfach nicht vertraut und um Schaden anzurichten, reicht ein Mitarbeiter mit böswilligen Absichten vollkommen aus.

Sie benötigen eine Möglichkeit zur Durchsetzung der Richtlinien, die Ihrem Unternehmen umfassenden Schutz bieten – denn blindes Vertrauen könnte schwerwiegende Folgen haben. Sie benötigen Novell ZENworks Endpoint Security Management, um für die kontinuierliche Durchsetzung von Richtlinien zu sorgen.

Und zwar jedes Mal.

Die Richtlinien können von Ihnen jederzeit geändert werden ,doch Ihre Benutzer haben keinen Einfluss darauf. Und genau das ist entscheidend: Die Bedrohung durch die Benutzer wird minimiert. Denn durch die Richtlinie wird Sicherheit gewährleistet.

Fehler wiedergutmachen

Benutzer machen Fehler. Manchmal wird beispielsweise ein Notebook am Flughafen vergessen. Obwohl der Verlust eines Geräts oftmals ärgerlich und teuer ist, sind die weitaus wertvolleren Daten, die im Gerät gespeichert sind, mit Micro Focus ZENworks Full Disk Encryption für den nächsten Besitzer des Notebooks nicht entzifferbar. Mit Full Disk Encryption müssen Sie sich keine Sorgen darüber machen, wo auf der Festplatte Daten gespeichert sind – alles ist verschlüsselt.

Der Verlust eines Passwort ist zwar weitaus banaler, kommt aber viel häufiger vor. Mit anderen Verschlüsselungssoftwares ist dies nicht nur ein weiterer Tag, den man mit Helpdesk-Mitarbeitern verbringt. Ohne Passwort ist Ihre Festplatte so undurchdringlich wie ein Fels. Mit ZENworks ist dies nur ein simpler Helpdesk-Vorgang. Helfen Sie dem Benutzer dabei, sein Passwort zurückzusetzen oder verwalten Sie das Gerät selbst: Egal, welchen Weg Sie wählen, Sie werden von der Verschlüsselung, die die Daten schützt, nicht behindert.

Es ist Mittwoch, 8:00 Uhr morgens. Wissen Sie, was einer Ihrer Mitarbeiter im zweiten Stock gerade auf seinen USB-Stick herunterlädt? Wird sich Ihr auf Reisen befindlicher CFO daran erinnern, sein Notebook mit an Bord zu nehmen?

Umfassender Schutz

Micro Focus Novell ZENworks Endpoint Security Management ist die ideale Lösung zur Durchsetzung von Richtlinien auf Endgeräten. Das Produkt „kennt“ Ihre Benutzer und weiß, welche Aktivitäten sie durchführen dürfen und welche nicht. Ein weiteres, einzigartiges Merkmal von Novell ZENworks Endpoint Security Management ist die standortabhängige, dynamische Anpassung der Sicherheitsstufe.

Wenn Sie die richtlinienorientierte Leistung von Endpoint Security Management mit der Absicherung durch Full Disk Encryption kombinieren, können Sie sich entspannt zurücklehnen, da externe Hacker nicht zugreifen und Schäden anrichten können. Dies schützt Mitarbeiter, die nur ihrer Arbeit nachgehen möchten. Ihre Daten sind sicher.

Produktivität und Sicherheit

Mit Novell ZENworks Endpoint Security Management finden Sie die goldene Mitte zwischen Produktivität und Sicherheit. Mit ZENworks Endpoint Security Management und ZENworks Full Disk Encryption können Sie:

- Dynamischen Schutz mithilfe von benutzer- und standortabhängigen Sicherheitsstufen sowie schnelle Anpassung von Richtlinien (z. B. bei Wi-Fi-Verbindungen) anwenden
- Daten auf mobilen Geräten verschlüsseln
- strenge Richtlinien zum Schutz vor Datenmissbrauch durchsetzen, z. B.

Festlegung von zugelassenen und verbotenen USB-Geräten

- alle Ressourcen, die Ihre Mitarbeiter für ihre tägliche Arbeit benötigen bereitstellen, ohne Sicherheitslücken offen zu lassen

Unantastbare Sicherheit

ZENworks Endpoint Security Management ist die ideale Lösung für die Durchsetzung Ihrer Richtlinien. Sie ist weder bestechlich noch lässt sie sich einschüchtern – und das Beste: Sie schläft nie. ZENworks Endpoint Security Management sorgt für die zuverlässige Durchsetzung Ihrer Richtlinien – tagaus, tagein.

Es ist Mittwoch, 8:00 Uhr morgens. Wissen Sie, was einer Ihrer Mitarbeiter im zweiten Stock gerade auf seinen USB-Stick herunterlädt? Wird sich Ihr auf Reisen befindlicher CFO daran erinnern, sein Notebook mit an Bord zu nehmen?

Wenn Sie über ZENworks Endpoint Security Management und ZENworks Full Disk Encryption verfügen, müssen Sie sich darüber keine Sorgen machen.

Über Micro Focus

Seit 1976 hat Micro Focus mehr als 20.000 Kunden unterstützt, indem sie Lösungen schaffen, die etablierte Technologien mit modernen Funktionen verknüpfen. Die beiden Portfolios verfolgen eine klare Vision – die Bereitstellung innovativer Produkte mit herausragendem Kundendienst. **www.microfocus.com**

„Wir suchten nach einer Lösung, die unser Netzwerk vor Viren, Hackern und anderen Bedrohungen schützen würde. Mit Novell (jetzt Teil von Micro Focus) ZENworks Endpoint Security Management profitieren wir von besonders umfassendem Schutz: Unsere mobilen Benutzer erhalten den erforderlichen flexiblen Fernzugriff, und wir können uns darauf verlassen, dass unser Netzwerk sicher ist.“

LAURA DAVIS
Technology Lead
Woolpert, Inc.

„Schon allein der ROI von Novell (jetzt Teil von Micro Focus) ZENworks Endpoint Security Management ist überzeugend. Wenn wir damit auch nur einen Fall von Datenmissbrauch vermeiden, können wir u. U. drei Millionen US-Dollar an Verfahrenskosten sparen.“

ROBB PETTIGREW
Manager, Technical Systems and Help Desk
Wyoming Medical Centre

Micro Focus
Deutschland
Fraunhoferstraße 7
D-85737 Ismaning
+49 89 42094 0

Micro Focus
Schweiz
Flughafenstrasse 90
CH-8058 Zürich-Flughafen
+41 43 456 2300

Micro Focus
Firmenhauptsitz
Vereinigtes Königreich
+44 (0) 1635 565200

www.novell.com