chrome enterprise

Unternehmenssicherheit in der Cloud

Organisationen geben viel Geld für Produkte aus, die angeblich Sicherheitslücken erkennen und Hackerangriffe sowie Spionagesoftware fernhalten. Doch trotz dieser Sicherheitsbemühungen steigt die Zahl an Datenlecks kontinuierlich.

> Prognosen aus dem Jahr 2019 gehen von einem Marktanstieg im Bereich Datenschutz **von 8,7 % auf 124 Milliarden $ aus**[1]

> Gleichzeitig steigt die Zahl großer, zielgerichteter Angriffe auf Datenbanken in den USA **jährlich um mehr als 27 %**[2]

Anzahl und Komplexität der Attacken nehmen zwar zu, die Vorgehensweisen bei diesen Angriffen an sich sind aber bereits bekannt: vorrangig Malware, Ransomware und Phishing. Offensichtlich sind die herkömmlichen Schutzmechanismen nicht mehr effektiv. Es ist also an der Zeit, neue Lösungen für dieses alte Problem zu finden.

Einzigartiger Ansatz in Bezug auf Endpunktsicherheit mit Chrome Enterprise

Gerätesicherheit auf mehreren Ebenen

Auf dem Chromebook arbeiten alle Ebenen zusammen, dadurch entsteht ein einzigartiger Schutzmechanismus.

- Nutzerdaten verschlüsseln
- Manipulation des Betriebssystems verhindern
- Datenspeicherung auf dem Gerät reduzieren
- Regelmäßige Patches und Updates durchführen
- Nutzer vor fahrlässigen Aktionen schützen

Isolierte und verwaltete Apps

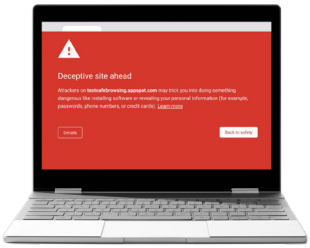
Schädliche Apps können von Nutzern nicht installiert werden.

- Potenzielle Angriffsflächen durch Sandboxes einschränken
- Zugriffsrichtlinien erzwingen
- Mehrere sichere Systeme anbieten, z. B. Chrome Web Store, Google Play, Web und native Linux-Apps

[1] Ponemon and Accenture, 2017; [2] Gartner, 2018

chrome enterprise

Unternehmen vor bekannten Gefahren schützen – mit Chrome Enterprise und Google Cloud



Phishing

Dank Google Safe Browsing werden Nutzer vor schädlichen Websites gewarnt, bevor sie sie aufrufen.

Sicherheitsschlüssel und die Bestätigung in zwei Schritten verhindern, dass Hacker gestohlene Passwörter verwenden können.

Im Falle eines Angriffs: Aufgrund der Richtlinie für Passwort-Warnungen müssen Nutzer ihr Passwort ändern, wenn es auf einer nicht autorisierten Website verwendet wurde.

Ransomware

Dadurch, dass nur wenige Daten auf dem Gerät gespeichert werden, ist der Umfang an Daten begrenzt, die Erpresser nutzen könnten.

Schreibgeschützte Betriebssysteme verhindern, dass ausführbare Dateien lokal ausgeführt werden.

Im Falle eines Angriffs: Bestätigter Bootmodus: Beim Start wird bestätigt, dass das System nicht modifiziert wurde.

Schädliche Apps

Über schwarze Listen, die auf Berechtigungen basieren, wird der Zugriff auf Erweiterungen geregelt.

Managed Google Play erleichtert die Auswahl nach Nutzergruppe und Richtlinienkonfiguration pro App.

Im Falle eines Angriffs: Durch Sandbox-Technologie wird die Angriffsflächen minimiert.

Darum benötigen Chromebooks keinen Virenschutz

Schreibgeschützt: Installierte Apps und Erweiterungen können keine Änderungen am Betriebssystem vornehmen.

Weil Software in einer Sandbox ausgeführt wird, werden Angriffe auf einer eingeschränkten Oberfläche isoliert.

Der bestätigte Bootmodus verhindert das Starten manipulierter Geräte.

Für alle Erweiterungen und Apps ist ein **Überprüfungsprozess erforderlich.**

Darum sind Chromebook-Updates so effektiv

Keine Ausfallzeiten: Updates finden im Hintergrund statt, während der Nutzer weiterarbeiten kann.

Zwei Versionen des Betriebssystems auf dem Gerät sorgen dafür, dass immer eines verwendet werden kann, während das andere aktualisiert wird.

Updates werden beim Neustart angewendet und innerhalb von Sekunden fertiggestellt.

Weitere Informationen zur Sicherheit bei Chrome Enterprise:
cloud.google.com/chrome-enterprise/security

© 2019 Google LLC. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.