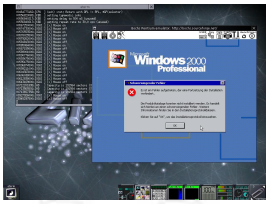

Leichtes Spiel für Hacker: Die 5 häufigsten Konfigurationsfehler

Auch wenn Cyberkriminelle immer anspruchsvollere Angriffstechniken nutzen, um in Unternehmensnetzwerke einzudringen – oft sind Sicherheitsverletzung auf vermeidbare, häufig übersehene Fehlkonfigurationen zurückzuführen. Um Hackern nicht Tür und Tor auf sensible Daten und IT-Umgebungen zu öffnen, im Folgenden deshalb die fünf häufigsten Konfigurationsfehler, die es für Unternehmen zu vermeiden gilt.

1. Standard-Anmeldeinformationen

Nicht konfigurierte Standard-Benutzernamen und -Passwörter von Geräten, Datenbanken, und Installationen sind vergleichbar mit dem Hinterlassen des Schlüssels in einer verschlossenen Tür. Selbst Hobbyhacker können hier mithilfe frei verfügbarer Tools einem Unternehmen weitreichenden Schaden zufügen. Standard-Anmeldedaten auf Netzwerkgeräten wie Firewalls, Routern oder sogar Betriebssystemen ermöglicht es Angreifern, simple Passwort-Checkscanner zu verwenden, um einen direkten Zugang zu erhalten. Bei etwas ausgeklügelteren Attacken führen Hacker eine Reihe von Skriptangriffen aus, um Geräte mit roher Gewalt zu knacken, indem sie sich entweder auf Standardbenutzernamen und -passwörter oder einfache Kennwörter wie "qwerty" oder "12345" konzentrieren.

2. Mehrfachverwendung von Passwörtern

Werden in einer Flotte von Endpunkten auf jedem Gerät dasselbe Benutzerkonto und Passwort verwendet, gibt dies Cyberkriminellen die Möglichkeit, jede Maschine anzugreifen, selbst wenn nur eines der Geräte einen Sicherheitsverstoß erlitten hat. Von dort aus können Angreifer Credential-Dumping-Programme verwenden, um die Passwörter oder sogar die Hashes selbst in die Finger zu bekommen. Unternehmen sollten deshalb die Wiederverwendung von Passwörtern um jeden Preis vermeiden und nicht benötigte Konten deaktivieren.

3. Offene Remote Desktop Services und Standard-Ports

Dienste wie Remote Desktop Protocol (RDP), ein von Microsoft entwickeltes proprietäres Protokoll, bieten Administratoren eine Schnittstelle zur Fernsteuerung von Computern. Zunehmend haben Cyberkriminelle dieses offene Protokoll missbraucht, wenn es nicht richtig konfiguriert war. Beispielsweise kann Ransomware wie CrySiS und SamSam Unternehmen über offene RDP-Ports ansprechen, sowohl durch Brute Force als auch durch Dictionary-Angriffe. Jedes nach außen gerichtete Gerät, das mit dem Internet verbunden ist, sollte deshalb durch einen mehrschichtigen Schutz abgesichert werden, um Zugriffsversuche wie etwa einen Brute-Force-Angriff zu bekämpfen. Administratoren sollten eine Kombination aus starken, komplexen Passwörtern, Firewalls und Zugriffskontrolllisten nutzen, um die Wahrscheinlichkeit eines Sicherheitsverstoßes zu reduzieren.

4. Verzögertes Software-Patching

Oft machen Zero-Day-Bedrohungen Schlagzeilen, doch die häufigsten Schwachstellen, die durch Cyberkriminelle ausgenutzt werden, sind in der Regel digitale Fossilien. Daher ist die Aktualisierung von Betriebssystemen und Patches entscheidend, um einen Sicherheitsverstoß zu verhindern. Auch wenn täglich zahlreiche Exploits und Schwachstellen gefunden werden und es schwierig sein kann, Schritt zu halten, gilt es für Unternehmen, verzögertes Software-Patching zu vermeiden.

5. Ausgeschaltete Protokollierung

Deaktiviertes Logging erlaubt es Angreifern nicht unbedingt, in ein System einzudringen, aber es ermöglicht ihnen, dort unbemerkt zu agieren. Einmal eingedrungen, können sich Hacker seitlich durch das Netzwerk bewegen, um nach Daten oder Assets zu suchen, die sie hinausschleusen wollen. Ohne entsprechende Protokollierung hinterlassen sie dabei keine Spuren. Dies schafft eine Nadel im Heuhaufen für IT-Teams bei der Rekonstruktion eines Sicherheitsvorfalls. Daher sollte die Protokollierung aktiviert sein und an einen zentralen Ort wie eine SIEM-Plattform (Security Information and Event Management) gesendet werden. Diese Daten liefern die Spuren, die forensische Analysten während einer Incident-Response-Untersuchung benötigen, um den Angriff nachzuvollziehen und den Einbruch zu erfassen. Darüber hinaus hilft dies, adäquat auf Bedrohungen zu reagieren, die eine Warnung aufgrund bereits protokollierter Ereignisse auslösen.

Durch Fehlkonfigurationen und das Belassen von Geräten oder Plattformen in ihrem Standardzustand haben Cyberkriminelle leichtes Spiel bei ihren Angriffen. Deshalb sollten Unternehmen die oben genannten Sicherheitsmaßnahmen implementieren, um sich und ihre sensiblen Daten zu schützen.