Versteckte Cyberbedrohungen: Linux-Backdoors im Visier der Hacker – Wie Unternehmen jetzt handeln sollten

Utl.: Aktuelle Bedrohungsszenarien erkennen und handeln – bewährte Tipps zum Computer Security Day 2024

(Wien, 30.11.2024) Cyberangriffe haben sich in den letzten Jahren stark gewandelt: Hacker nehmen inzwischen vermehrt Linux-Server und -Geräte ins Visier, nachdem frühere Schwachstellen in Windows-Systemen zunehmend geschlossen wurden. Laut einem aktuellen Bericht von ESET, einem führenden Anbieter von IT-Sicherheitslösungen, hat die Hackergruppe Gelsemium neuartige Linux-Backdoors entwickelt, die herkömmliche Schutzmechanismen umgehen und so unbemerkt IT-Netzwerke infiltrieren können. Diese Entwicklung zeigt: Kein Betriebssystem ist vor Angriffen sicher.

Die Bedrohung betrifft nicht nur kritische Infrastrukturen oder große Konzerne – auch kleine und mittelständische Unternehmen stehen zunehmend im Fokus der Angreifer. Denn gerade dort mangelt es oft an den notwendigen Schutzmaßnahmen.

Marco Gschaider, CEO und IT-Security-Experte bei Iphos IT Service, warnt: „Die Bedrohung ist real und verschärft sich kontinuierlich. Gerade die Nutzung von Linux-Backdoors durch Gruppen wie Gelsemium zeigt, wie wichtig ein mehrstufiger Schutz von Unternehmensnetzwerken ist."

Neue Backdoors: Warum Unternehmen jetzt handeln müssen

Die von ESET entdeckten neuen Backdoors verdeutlichen, wie gezielt Angreifer Sicherheitslücken nutzen, um unerkannt in Netzwerke einzudringen. Diese Entwicklungen sind nicht nur ein Weckruf für große Unternehmen, sondern auch für KMUs, die oft nicht über ausreichende Sicherheitsmaßnahmen verfügen. „Angriffe wie diese treffen häufig diejenigen am härtesten, die glauben, nicht im Fokus der Hacker zu stehen", erklärt Gschaider.

Laut einer aktuellen Analyse wurden über 60 % der entdeckten Sicherheitslücken in den letzten zwei Jahren nicht durch Angriffe, sondern durch proaktive Sicherheitschecks gefunden – ein klares Signal, dass Prävention der Schlüssel ist.

So können sich Unternehmen vor Cyberangriffen schützen

1. Patch-Management: Die Basis einer sicheren IT

Regelmäßige Updates und Patches sind die Basis jeder IT-Sicherheitsstrategie. Hacker greifen oft auf Schwachstellen zurück, die längst bekannt sind, aber nicht geschlossen wurden. „Unternehmen, die ihre Systeme regelmäßig aktualisieren, können bis zu 85 % der bekannten Cyberangriffe abwehren", erklärt Marco Gschaider und nennt ein Beispiel: „Die vor einigen Jahren bekannt gewordene Sicherheitslücke EternalBlue, die von WannaCry ausgenutzt wurde, konnte durch

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347

ein einfaches Windows-Update geschlossen werden.“ Ein zuverlässiges Patch-Management stellt sicher, dass solche Updates automatisch und zeitnah durchgeführt werden, ohne den laufenden Betrieb zu stören. Eine unkomplizierte Methode zur Stärkung der Resilienz im Unternehmen ist der Einsatz des Vulnerability und Patch Management Tools von ESET. Aufgrund der aktuellen Bedrohungsszenarien wurde dieses nun auch für Linux und macOS erweitert.

2. Frühwarnsystem für Hackerangriffe: Wie ein Intrusion-Detection-System (IDS) hilft

Ein Intrusion-Detection-System ist wie ein Frühwarnsystem für die IT eines Unternehmens. Es überwacht den Netzwerkverkehr und meldet verdächtige Aktivitäten – etwa, wenn ein Angreifer versucht, Zugriff auf Server zu erhalten oder ungewöhnliche Datenmengen aus dem Netzwerk gesendet werden. So kann ein IDS beispielsweise auffällige Login-Versuche aus ungewöhnlichen Ländern erkennen und Alarm auslösen, bevor ein Angriff erfolgreich wird. „Mit einem IDS können Angriffe oft gestoppt werden, bevor sie Schäden anrichten“, so Gschaider. Der Unterschied zu herkömmlichen Sicherheitsmaßnahmen? Ein IDS arbeitet in Echtzeit und ergänzt damit den Schutz durch Antiviren-Software und Firewalls.

3. IT-Check-ups: Schwachstellen finden, bevor es zu spät ist

Sicherheitsaudits sind eine Vorsorgeuntersuchung, ein Check-up für Ihre IT-Infrastruktur. Dabei werden nicht nur technische Schwachstellen wie ungesicherte Server oder veraltete Software geprüft, sondern auch organisatorische Risiken. Denn oft sind schwache Passwörter oder falsch konfigurierte Benutzerrechte der Einstiegspunkt für Angreifer. Ein Audit deckt solche Risiken auf und hilft Unternehmen, ihre Sicherheitsmaßnahmen gezielt zu verbessern. „Das Ziel eines Audits ist nicht, Schuldige zu finden, sondern Schwächen zu erkennen, bevor sie ausgenutzt werden können“, betont Gschaider.

4. Angriffsfläche minimieren: Server-Härtung für mehr Sicherheit

Bei der Server-Härtung geht es darum, unnötige Funktionen und Dienste auf einem Server zu deaktivieren und so die Angriffsfläche für potenzielle Hacker zu minimieren. Ein Beispiel: Ein Unternehmensserver, der über Dienste wie FTP oder Telnet verfügt, die nicht genutzt werden, bietet Angreifern einen möglichen Einstiegspunkt ins Unternehmensnetz. Durch die Entfernung solcher überflüssigen Funktionen wird das Risiko deutlich reduziert. „Eine gehärtete Serverstruktur ist wie ein Haus ohne unnötigen Hintertüren – es gibt weniger Möglichkeiten für Einbrecher hineinzugelangen“, erklärt Gschaider.

Der Computer Security Day - ein Anlass zum Handeln

Der Computer Security Day ist eine gute Gelegenheit, sich mit der eigenen IT-Sicherheit auseinanderzusetzen. Gschaider betont: „Gerade kleinere Unternehmen unterschätzen oft, wie leicht sie Ziel von Angriffen werden können. Dabei ist

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347

Prävention einfacher und günstiger, als die Folgen eines erfolgreichen Angriffs zu beheben."

Als ESET Platinum Partner unterstützt Iphos IT Service Unternehmen jeder Größe bei der Entwicklung und Umsetzung maßgeschneiderter Sicherheitsstrategien. Egal ob es um die Implementierung von Intrusion-Detection-Systemen, die effiziente Planung von Sicherheitsupdates, Server Härtung oder andere IT-Security Themen geht - wir helfen Unternehmen dabei, IT-Sicherheitsmaßnahmen optimal einzusetzen und so die Resilienz gegen Cyberangriffe zu stärken.

Über Iphos IT Service GmbH

Iphos IT Service GmbH ist ein internationales Unternehmen, das Dienstleistungen in den Bereichen IT-Infrastruktur, IT-Wartung und IT-Consulting anbietet. 2019 aus der bereits 1998 in Wien gegründeten Iphos IT Solutions GmbH hervorgegangen, betreibt Iphos IT Service einen weiteren Standort in Bulgarien (Sofia). Die Dienstleistungen werden in Österreich, Deutschland, der Schweiz und Bulgarien vertrieben. Ing. Christoph Wendl leitet gemeinsam mit Marco Gschaider als Chief Executive Officer (CEO) das Unternehmen, das sich mit innovativen Lösungen den aktuellen Herausforderungen der IT stellt.

Rückfragehinweis für Medien:
Marco Gschaider
Geschäftsführer, Iphos IT Service GmbH
Khekgasse35
1230 Wien
Tel.: +43 1 869 84 00
E-Mail: marketing@iphos.com
https://www.iphos.com

Iphos IT Service GmbH
Khekgasse 35
A-1230 Wien

+43 1 869 84 00
+43 1 869 84 00 50
office@iphos.com
iphos.com

Erste Bank, BIC: GIBAATWW
IBAN: AT602011184095568000
CEO: Ing. Christoph Wendl,
Marco Gschaider,
Handelsgericht Wien, Sitz Wien
FN 513426p,
ATU74517347