Microsoft war Top-Köder für Phishing in Q3/2020

Berichte der Sicherheitsforscher von Check Point zeigen klar, das Cyberkriminelle aktuell für Phishing am häufigsten den Tech-Riesen Microsoft imitieren. Entgegen kommt ihnen dabei der Trend „Fernzugriff".

San Carlos, Kalifornien – 20. Oktober 2020 – Die Sicherheitsforscher von Check Point® Software Technologies Ltd. (NASDAQ: CHKP) haben ihre Ergebnisse des „Brand Phishing Reports" für das dritte Quartal offengelegt. Darin verzeichnete sich ein klarer Trend unter den Cyberkriminellen: Microsoft ist aktuell das für Phishing am meisten imitierte Unternehmen (Marke).

Mit der zweiten großen Welle der Corona-Pandemie in Deutschland hat sich ein Großteil der Arbeiterschaft in Unternehmen erneut öfter im Home Office wiedergefunden – ein Umstand, den sich Phishing-Betrüger zu Nutze machen. Unter dem Deckmantel von Microsoft versuchen die Cyberkriminellen, unbedarfte Mitarbeiter im Home Office hereinzulegen, die sich aktuell erhöhter Eigenverantwortung in Sachen IT-Betrieb, Fernzugriffen und Patches gegenüber sehen. 44 Prozent der Betrugsversuche werden dabei per Mail verteilt, 43 Prozent sind Fallen im Netz und 12 Prozent zielen auf mobile Endgeräte. Während Microsoft im vergangenen Quartal noch lediglich in 7 Prozent der Fällen als Köder genutzt wurde und damit auf Platz fünf der imitierten Unternehmen lag, sind es nun 19 Prozent und Platz eins. Die Top-Zehn gestaltet sich wie folgt:

1. Microsoft (in 19 % aller „Marken"-Phishing-Versuche weltweit)
2. DHL (9 %)
3. Google (9 %)
4. PayPal (6 %)
5. Netflix (6 %)
6. Facebook (5 %)
7. Apple (5 %)
8. Whatsapp (5 %)
9. Amazon (4 %)
10. Instagram (4 %)

Christine Schönig, Regional Director Security Engineering CER, Office of the CTO bei Check Point Software Technologies GmbH, warnt daher: „Mitarbeiter im Homeoffice sind eine Anlaufstelle für Hacker. Weltweit lassen Unternehmen ihre Mitarbeiter wegen der Coronavirus-Pandemie von Zuhause aus arbeiten, möglicherweise zum ersten Mal überhaupt. Der plötzliche Wandel hat viele Unternehmen und Mitarbeiter kalt erwischt – es mangelt an konkreter Vorbereitung auf die jüngsten Cyberangriffe. Hacker, die eine große Chance wittern, imitieren die für die Arbeit der Angestellten bekannteste Marke: Microsoft. Ich gehe davon aus, dass die Nachahmung von Microsoft auch im neuen Jahr anhalten wird. Ich ermutige die Angestellten im Homeoffice besonders vorsichtig zu sein, wenn sie eine E-Mail erhalten. Besonders dann, wenn es in der Mail um ihr 'Microsoft'-Konto geht."

Um die Gefahr im Homeoffice zu reduzieren hat Check Point folgende Tipps für Angestellte:

1. **Lernen Sie die sogenannten „roten Flaggen" kennen**. Es gibt bestimmte Merkmale (rote Flagge), die einen Angriff durch eine E-Mail verraten können. Einige der roten Flaggen sind: schlechte Formatierung, Rechtschreib- und Grammatikfehler und allgemeine Begrüßungen wie „Lieber

Benutzer“ oder „Lieber Kunde“. Stellen Sie sicher, dass Links mit https:// und nicht mit http:// beginnen. Vertrauen Sie niemals alarmierenden Nachrichten.

2. **Vermeiden Sie die übermäßige Weitergabe von Informationen**. Als allgemeine Faustregel gilt: Teilen Sie nur das Nötigste, unabhängig davon, auf welcher Website Sie sich befinden. Unternehmen benötigen niemals Ihre Sozialversicherungsnummer oder Ihr Geburtsdatum, um mit Ihnen Geschäfte zu machen. Geben Sie Ihre Zugangsdaten niemals an Dritte weiter.
3. **Löschen Sie verdächtige E-Mails**. Wenn Sie glauben, dass etwas nicht stimmt, ist es wahrscheinlich auch so. Löschen Sie verdächtige E-Mails, ohne sie zu öffnen oder auf irgendwelche Links zu klicken, und leiten Sie sie zur Untersuchung an die IT-Abteilung weiter. Gehen Sie nach Ihrem Bauchgefühl.
4. **Klicken Sie nicht auf Anhänge**. Öffnen Sie keine Anhänge in diesen verdächtigen oder seltsamen E-Mails – insbesondere keine Word-, Excel-, PowerPoint- oder PDF-Anhänge.
5. **Überprüfen Sie den Absender**. Bei jeder E-Mail, die Sie erhalten, müssen Sie genau nachschauen, wer sie versendet. Wer oder was ist die Quelle der E-Mail? Gibt es Rechtschreibfehler in der E-Mail-Domäne? Achten Sie auf Rechtschreibfehler oder Änderungen in den E-Mail-Adressen des E-Mail-Absenders. Zögern Sie nicht, verdächtige E-Mail-Absender über Ihren E-Mail-Client zu blockieren.
6. **Halten Sie Ihre Geräte und Software auf dem neuesten Stand**. Stellen Sie sicher, dass alle Ihre Anwendungen auf Ihrem Mobiltelefon und Desktop-Computer über die neuesten Software-Versionen verfügen. Diese Versionen verfügen über die neuesten Schwachstellen-Patches und Abwehrmechanismen, damit Sie sicher sind. Die Verwendung veralteter Software kann Hackern Tür und Tor öffnen, um an Ihre persönlichen Daten zu gelangen.

Den kompletten Bericht über Marken-Phishing-Versuche im dritten Quartal 2020 lesen Sie unter: https://blog.checkpoint.com/2020/10/19/microsoft-is-most-imitated-brand-for-phishing-attempts-in-q3-2020/

Alle Berichte von Check Point finden Sie unter: https://blog.checkpoint.com/
Alle Berichte des Check Point Research Teams finden Sie unter: https://research.checkpoint.com/

Folgen Sie Check Point auf:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Folgen Sie Check Point Research hier:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

Über Check Point Research
Check Point Research bietet führende Cyber-Bedrohungsinformationen für Check Point Software-Kunden und die größere Intelligenz-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die auf der ThreatCloud gespeichert sind, um Hacker fernzuhalten und gleichzeitig sicherzustellen, dass alle Check Point Produkte mit den neuesten Schutzmaßnahmen aktualisiert werden. Das Forschungsteam besteht aus über 100 Analysten und Forschern, die mit anderen Sicherheitsanbietern, der Strafverfolgung und verschiedenen CERTs zusammenarbeiten.

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Die Lösungen schützen Kunden vor Cyber-Angriffen der 5. Generation mit einer branchenführenden Fangrate von Malware, Ransomware und anderen gezielten Angriffen. Check Point bietet die mehrstufige Sicherheitsarchitektur ‚Infinity' Total Protection mit Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Operationen eines Unternehmens, sowie die Geschäftsinformationen auf diesen Geräten, vor allen bekannten Angriffen schützt. Check Point liefert zudem das umfassendste und intuitivste Single Point of Control Management-System der Branche. Check Point schützt über 100.000 Unternehmen jeder Größe in der ganzen Welt. Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt rund 50 Mitarbeitende.

Pressekontakt:
Check Point Software Technologies (Switzerland) AG
Sonja Meindl
Tel: +41 44 316 64 44
E-Mail: smeindl@checkpoint.com

Jenni Kommunikation
Oliver Schneider
Tel: +41 44 388 60 80
E-Mail: oliver.schneider@jeko.com

