Panda Security

Gefährlicher Online-Fischzug: Wie schützt man sich vor Pharming?

***Duisburg, 15. November 2022* – Kein Zugriff auf das Mailpostfach, der Bezahldienst verweigert den Zugang und auf dem Bankkonto erscheinen unbekannte Transaktionen – dann sind Sie wahrscheinlich Opfer von Pharming, einer neuen Technik, mit der Hacker auf sensible Daten zugreifen. Um was es sich dabei genau handelt und wie Sie sich und Ihre Geräte vor der Masche schützen können – Softwareanbieter Panda Security gibt hilfreiche Tipps.**

Der Name Pharming setzt sich aus den Begriffen „Farming“ und „Pishing“ zusammen und beschreibt eine Cyberangriffmethode, bei der Nutzer ohne ihr Wissen oder ihre Zustimmung auf gefälschte Websites umgeleitet werden. Der bösartige Code ändert die IP-Adressdaten und lockt Nutzer so auf Schein-Websites, wo sie persönliche Daten eingeben. Diese werden dann für Identitätsdiebstahl oder Finanzbetrug verwendet. Pharming-Angriffe zielen daher vor allem auf Kunden von Banken oder anderen Geldwechseldiensten. Dies ermöglicht Hackern zudem, gleich mehrere Geräte auf einmal zu infiltrieren.

Wie funktioniert Pharming?

Beim Pharming werden entweder einzelne Computer oder ein ganzer Server infiziert. Zwar werden in beiden Fällen Websites umgeleitet, das Vorgehen ist jedoch unterschiedlich.

Hacken einzelner Computer: Bei dieser Art von Pharming verschickt der Hacker eine E-Mail mit einem Code, der die Hostdateien eines Computers verändert. Sind die Dateien infiltriert, werden Nutzer auf eine gefälschte Version der Website umgeleitet. Selbst wenn ein Nutzer die richtige URL eingibt, landet er automatisch auf der Fälschung. Die gefälschte Website ahmt Design und Optik einer echten Website nach und erweckt den Glauben, auf einer sicheren Seite zu sein.

Hochgradige Infektionsgefahr durch DNS-Poisoning: Eine weitaus extremere Form des Pharming ist das Infizieren des DNS-Servers (DNS-Poisoning). DNS-Server übersetzen im Wesentlichen Domänennamen in IP-Adressen, wobei sie zwischen „menschlicher“ und „Computer“-Sprache wechseln.

Bei dieser Form des Pharming ist der DNS-Server Ziel des Hackers, anstatt Dateien auf einzelnen Computern zu infiltrieren. Server können Tausende bis Millionen von URL-Anfragen von Internetnutzern verarbeiten, so dass jeder Nutzer unwissentlich auf gefälschte Seiten umgeleitet wird. Diese groß angelegte Attacke ist besonders gefährlich, da betroffene Nutzer trotz eines sicheren und malwarefreien persönlichen Computers zu Opfern werden können.

Wie erkennt man einen Pharming-Angriff?

Pharming-Angriffe sind schwer zu erkennen, vor allem, wenn die gefälschte Website kaum vom Original zu unterscheiden ist. Es gibt jedoch kleine Tricks, um einen Angriff zu erkennen und abzuwehren. Einige häufige Anzeichen für Pharming, auf die Sie achten sollten, sind:

- **Geringfügige Änderungen an einem Link oder einer Website**
  Angreifer ändern bei der Erstellung gefälschter Seiten manchmal Buchstaben in der URL oder Grafiken. Wenn Sie beim Besuch einer vertrauten Website Tippfehler, unbekannte Logos oder Farben bemerken, könnte es sich um eine Pharming-Website handeln.
- **Unsichere Verbindung**
  Pharming-Websites verwenden oft „http“ statt „https“ in der URL, was auf eine unsichere Verbindung hinweist. Wenn eine Warnmeldung auf eine unsichere Verbindung hinweist, oder kein graues Vorhängeschloss-Symbol in der Adressleiste erscheint, handelt es sich möglicherweise um eine bösartige Website.
- **Ungewöhnliche Konto- oder Bankaktivitäten**
  Angreifer nutzen häufig Pharming, um auf Bankkonten und sensible Informationen zuzugreifen. Unzulässige Aktivitäten auf dem Kreditkarten- oder Bankkonto deuten möglicherweise auf einen Pharming-Angriff hin.
- **Unbefugte Passwortänderungen**
  Erhält ein Angreifer Zugang zu Anmeldedaten für ein Online-Konto, ändert er möglicherweise das Kennwort, um dem Nutzer den Zugang zu verwehren. Zufällige Passwortänderungen sind ein guter Indikator für ein gehacktes Konto.
- **Unbekannte Apps oder Downloads**
  Unbekannte Apps oder Programme können ebenfalls auf einen Angriff verweisen.

Cybersecurity-Risiken

Pharming-Angriffe können sowohl für Unternehmen als auch für einzelne Nutzer schwerwiegende Folgen haben. Einige der häufigsten Risiken sind:

- **Datenverlust**
  Angreifer nutzen Pharming, um auf persönliche Daten oder andere sensible Informationen zuzugreifen. Dies ist besonders gefährlich bei sensiblen Daten im Business-Bereich oder bei Personen, die dasselbe Passwort für mehrere Online-Zugänge verwenden. Besteht der Verdacht, dass ein Angreifer durch einen Pharming-Angriff Zugang zu Anmeldedaten erlangt hat, müssen Passwörter sofort geändert und Sicherungsmaßnahmenergriffen werden.
- **Malware**
  Ein Klick auf unbekannte Links kann zur Installation von Viren und Malware führen. Ohne zuverlässiges Antivirenprogramm geschieht dies möglicherweise unbemerkt.
- **Diebstahl oder Finanzbetrug**
  Sobald ein Angreifer Zugang zu Konten erhält, kann er Geld stehlen oder betrügerische Einkäufe tätigen. Dies ist besonders häufig bei Fake-Websites der Fall, die sich als Banken oder vergleichbare Finanzinstitute ausgeben.

Wie man sich vor Angriffen schützen kann

Auch wenn sich viele Pharming-Angriffe nicht vollständig verhindern lassen, gibt es sinnvolle und effiziente Maßnahmen, um Cyberkriminelle abzuwehren:

- Löschen des DNS-Cache.
- Einsatz eines Antivirenprogramm wie Panda Dome.
- Bei dem Verdacht auf kompromitierte Server sollte der Internetdienstanbieter informiert werden.
- Installation eines VPN-Kanals für sicheres Online-Surfen.

Angesichts der weit verbreiteten räuberischen Taktiken wie Pharming und Phishing ist es wichtiger denn je, sich vor allen Arten von Malware-Angriffen zu schützen. Generelle Vorsichtsmaßnahmen und eine gute Anti-Viren-Software sind der erste Schritt.

Für verschiedene Anforderungen hat Panda Security vier verschiedene Pakete geschnürt: von „Panda Dome Essential“ mit Virenschutz, WLAN-Schutz vor Hackerangriffen und Virenscan für externe Geräte bis hin zu „Panda Dome Premium“ mit Schutz vor Viren, komplexen Onlineattacken, Premium VPN für anonymes Surfen sowie umfassendem Schutz von persönlichen Daten und Kennwörtern, Update-Manager und technischem Support rund um die Uhr.

Über Panda Security

Panda Security ist ein multinationales Unternehmen mit Hauptsitz in Spanien, das auf die Entwicklung von IT-Sicherheitslösungen spezialisiert ist. Zunächst auf Antivirensoftware fokussiert, hat das Unternehmen sein Geschäftsfeld inzwischen auf fortschrittliche Cyber-Security-Services ausgeweitet. Mit rund 600 Mitarbeitern agiert Panda Security in über 180 Ländern weltweit. Seit 2021 gehört Panda Security als hundertprozentige Tochtergesellschaft zu WatchGuard.

Weitere Informationen finden Interessierte unter https://www.pandasecurity.com/de/

Pressekontakt

Monika Brüggemann
Oliver Schrott Kommunikation GmbH
Friesenplatz 10
50672 Köln
pandasecurity@osk.de