PRINSOTEL

Handlungsempfehlungen für unsere Kunden nach der Cyber-Attacke vom 16. Mai 2024

Infolge des Angriffs ist es unsere Pflicht, Ihnen einige Richtlinien zur Verfügung zu stellen, um die Sicherheit Ihrer personenbezogenen Daten zu gewährleisten:

1. Wir werden Sie unter keinen Umständen auf elektronischem Wege nach Ihren Bankdaten fragen. Wenn Sie einen Anruf oder eine Nachricht erhalten, in der Sie um diese Art von Informationen gebeten werden, geben Sie diese NIEMALS weiter.

2. Wenn Sie PRINSOTEL-Werbung per E-Mail, SMS oder über soziale Netzwerke erhalten, **überprüfen Sie immer die Identität** des Absenders und klicken Sie im Zweifelsfall niemals auf einen Link, dem Sie nicht vertrauen.

3. **Seien Sie vorsichtig bei Anrufen in unserem Namen** oder von einem unserer Hotels. Vergewissern Sie sich, dass es sich um einen Anruf von einem bekannten Anbieter handelt und geben Sie niemals private Daten an.

Darüber hinaus möchten wir Sie mit diesem Dokument vor allen möglichen Betrugsversuchen infolge des Vorfalls warnen, wie z. B. Phising, Spear Phising, Vishing, Smising, Pharming, Whaling ... usw., damit Sie sich vor diesen bösartigen Handlungen schützen können.

Diese Arten von Angriffen oder Betrügereien werden im Folgenden detailliert beschrieben, damit Sie ein anormales Verhalten erkennen und solche Aktionen verhindern können:

- ***Phishing:*** Phishing ist eine Social-Engineering-Technik, bei der E-Mails verschickt werden, die die Identität von Unternehmen oder öffentlichen Einrichtungen vortäuschen und personenbezogene und Bankdaten des Benutzers anfordern. Über einen in der E-Mail enthaltenen Link wird versucht, den Benutzer auf eine betrügerische Website umzuleiten, auf der er seine Kreditkartennummer, Ausweisnummer, sein Passwort für den Zugang zum Online-Banking usw. eingeben muss.

  Diese betrügerischen E-Mails enthalten oft das Logo oder das Markenbild des Unternehmens, können grammatikalische Fehler enthalten und versuchen manchmal, Dringlichkeit und Angst zu vermitteln, um den Benutzer dazu zu bringen, die angeforderten Aktionen durchzuführen.
  Eine Phishing-E-Mail kann auch einen Anhang enthalten, der mit bösartiger Software infiziert ist. Das Ziel dieser Schadsoftware ist es, den Computer des Benutzers zu infizieren und vertrauliche Informationen zu stehlen.

- ***Spear Phishing:*** Angreifer erstellen gefälschte E-Mails, Webseiten und sogar Kurznachrichten, die authentisch aussehen und von den Nutzern Anmeldedaten verlangen. Auf diese Weise gelangen Betrüger in den Besitz von Anmeldedaten für Online-Shops, soziale Netzwerke oder Cloud-Speicherplätze. Im schlimmsten Fall gelangen sie sogar in den Besitz von Bankinformationen oder Kreditkartendaten. Die Betrüger wissen, dass viele Nutzer die Passwortsicherheit nicht ernst nehmen und dasselbe Passwort für verschiedene Dienste verwenden. Auf diese Weise kann eine einfache Phishing-Website genutzt werden, um an sensible Daten zu gelangen, die auf dem digitalen Schwarzmarkt einen hohen wirtschaftlichen Wert haben.

- ***Vishing:*** Der Begriff Vishing setzt sich aus den Wörtern Voice (Stimme) und Phishing zusammen, weshalb es auch manchmal als Voice-Phishing bezeichnet wird. Bei dieser Technik nutzen die Angreifer die VoIP-Technologie (Voice over IP), um zahlreiche billige oder kostenlose betrügerische Anrufe zu tätigen und so an Codes, Passwörter oder Bankdaten des oft ahnungslosen Opfers zu gelangen.

- ***Smishing:*** Der Begriff Smishing ist eine Kombination aus SMS und Phishing. Ähnlich wie beim Phishing geben sich die Cyberkriminellen, die diese Nachrichten verschicken, als Vertreter eines vertrauenswürdigen Unternehmens oder einer Organisation aus, aber statt E-Mails verwenden sie SMS (Short Message Service). Diese mobilen Nachrichten dienen entweder dazu, das Opfer zur Preisgabe von Kontodaten aufzufordern oder Malware und Trojaner auf dem Gerät des Opfers ohne dessen Wissen zu installieren.

- ***Pharming:*** Pharming, eine Kombination aus den Wörtern "Phishing" und "Farming", ist ein dem Phishing ähnlicher Online-Betrug, bei dem der Website-Verkehr manipuliert und sensible Informationen gestohlen werden. Dabei handelt es sich um eine Art von Social-Engineering-Cyberangriff, bei dem Kriminelle Benutzer, die auf eine bestimmte Website zugreifen wollen, auf eine andere, gefälschte Website umleiten. Diese "gefälschten" Websites versuchen, die personenbezogenen Daten und Anmeldeinformationen des Opfers wie Passwörter, Sozialversicherungsnummern, Kontonummern usw. abzufangen, oder versuchen, Pharming-Malware auf dem Computer des Opfers zu installieren.

- ***Whaling:*** Ein Whaling-Angriff ist eine Methode, mit der Cyberkriminelle vorgeben, eine leitende Position in einem Unternehmen einzunehmen, um leitende Angestellte oder andere wichtige Personen innerhalb des Unternehmens direkt anzugreifen, um Geld zu stehlen, vertrauliche Informationen zu erlangen oder sich zu kriminellen Zwecken Zugang zu ihren Computersystemen zu verschaffen. Whaling, auch als CEO-Betrug bekannt, ähnelt insofern dem Phishing, als es Methoden wie Website- und E-Mail-Spoofing einsetzt, um das Opfer unter anderem dazu zu bringen, vertrauliche Informationen preiszugeben oder Geld zu überweisen.

Es tut uns sehr leid, dass wir in diese Situation geraten sind, aber Sie sollten wissen, dass hre Sorgenfreiheit für uns an erster Stelle steht und wir die Situation schnell und effizient in den Griff bekommen haben.

Prinsotel arbeitet bereits an dem nach dem Vorfall erstellten Aktionsplan und insbesondere an der Umsetzung verstärkter Sicherheitsmaßnahmen, um ähnliche Situationen in Zukunft zu vermeiden.
