BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Phishing

Phishing ist eine weit verbreitete Technik von Cyberkriminellen, die gefälschte E-Mails oder Websites verwenden, um vertrauliche Informationen wie Passwörter, Kreditkartennummern oder andere persönliche Informationen zu stehlen.

ZIEL / SCHADEN

Phishing zielt darauf ab, sensible Daten zu stehlen, um finanziellen Betrug zu begehen, Identitäten zu stehlen oder Malware zu verbreiten. Diese Angriffe können erhebliche finanzielle und persönliche Schäden verursachen.

INFEKTIONSWEG

Phishing erfolgt in der Regel per E-Mail, in der sich betrügerische Links oder Anhänge befinden, oder über gefälschte Websites, die echten Websites täuschend ähnlich sehen.

ABWEHR

Seien Sie vorsichtig beim Umgang mit E-Mails oder Nachrichten von unbekannten oder unerwarteten Absendern, klicken Sie nicht auf verdächtige Links und öffnen Sie keine unbekannten Anhänge. Verwenden Sie stets aktuelle Antivirus-Software.

BEFREIUNG MÖGLICH?

Ja, indem Sie Ihre Daten sichern und Ihre Systeme regelmässig aktualisieren.

ANGRIFF - WAS NUN?

Wenn Sie Opfer eines Phishing-Angriff geworden sind, ändern Sie sofort Ihre Passwörter und überprüfen Sie Ihre Konten auf verdächtige Aktivitäten.

BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Ransomware

Ransomware ist eine bösartige Software, die Daten auf dem betroffenen Gerät verschlüsselt und den Benutzer dazu auffordert, ein Lösegeld zu zahlen, um wieder Zugriff auf die Daten zu erhalten. Die Verschlüsselung ist oft so stark, dass eine Entschlüsselung ohne den speziellen Schlüssel des Angreifers nahezu unmöglich ist.

ZIEL / SCHADEN

Ransomware zielt darauf ab, einen finanziellen Gewinn zu erzielen, indem sie den Zugriff auf die Daten eines Benutzers blockiert und ein Lösegeld für deren Freigabe verlangt. Die Schäden können erheblich sein, einschliesslich des Verlusts wichtiger Daten und finanzieller Verluste.

INFEKTIONSWEG

Ransomware kann über verschiedene Methoden verbreitet werden, darunter Spam-E-Mails, infizierte Software-Downloads oder Exploit-Kits, die Sicherheitslücken ausnutzen.

ABWEHR

Halten Sie Ihr Betriebssystem und Ihre Software stets auf dem neuesten Stand, um Sicherheitslücken zu schliessen. Verwenden Sie eine zuverlässige Sicherheitssoftware und führen Sie regelmässige Backups Ihrer wichtigen Dateien durch.

BEFREIUNG MÖGLICH?

In einigen Fällen können Entschlüsselungstools helfen, aber der sicherste Weg ist das Wiederherstellen der Daten aus einem Backup.

ANGRIFF - WAS NUN?

Zahlen Sie kein Lösegeld, da dies die Angreifer nur ermutigt. Wenden Sie sich an die Behörden und suchen Sie professionelle Hilfe und schliessen Sie eine Cyberversicherung ab.

BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Man-in-the-Middle

Ein Man-in-the-Middle-Angriff ist ein Cyberangriff, bei dem ein Angreifer die Kommunikation zwischen zwei Parteien abfängt, ohne dass diese davon wissen. Der Angreifer kann die Informationen abfangen, lesen, verändern und weiterleiten.

ZIEL / SCHADEN

Der Schaden kann erheblich sein, einschliesslich des Diebstahls persönlicher oder finanzieller Informationen, des Verlusts der Privatsphäre und potenzieller finanzieller Verluste.

INFEKTIONSWEG

Häufig treten Man-in-the-Middle-Angriffe auf, wenn Benutzer unsichere öffentliche WLAN-Netzwerke nutzen oder wenn Malware auf dem Gerät des Benutzers installiert ist.

ABWEHR

Nutzen Sie immer sichere und verschlüsselte Netzwerkverbindungen. Vermeiden Sie die Nutzung öffentlicher Wi-Fi-Netzwerke für sensible Transaktionen. Halten Sie Ihre Geräte und Anwendungen immer auf dem neuesten Stand.

BEFREIUNG MÖGLICH?

Ja, indem Sie Ihre Geräte regelmässig auf Malware überprüfen und sicherstellen, dass Ihre Kommunikation verschlüsselt ist.

ANGRIFF - WAS NUN?

Wenn Sie glauben, dass Sie Opfer eines Man-in-the-Middle-Angriffs geworden sind, ändern Sie sofort alle Ihre Passwörter. Überwachen Sie Ihre Konten auf ungewöhnliche Aktivitäten und informieren Sie die entsprechenden Institutionen über den Vorfall.

BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Social Engineering

Social Engineering ist eine Methode, bei der Manipulation und menschliche Interaktion genutzt werden, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben oder bestimmte Handlungen auszuführen.

ZIEL / SCHADEN

Social-Engineering-Angriffe können zu Datenverlusten, finanziellen Verlusten und Identitätsdiebstahl führen.

INFEKTIONSWEG

Meist über Kommunikationswege wie E-Mail, Telefon oder soziale Medien, wo der Angreifer sich als vertrauenswürdige Quelle ausgibt.

ABWEHR

Seien Sie vorsichtig bei der Preisgabe persönlicher Informationen und prüfen Sie die Authentizität von Anfragen. Bilden Sie Mitarbeiter in Sicherheitsbestimmungen und -protokollen aus.

BEFREIUNG MÖGLICH?

Ja, durch sofortige Änderung von Passwörtern und Überwachung von Konten auf ungewöhnliche Aktivitäten.

ANGRIFF - WAS NUN?

Wenn Sie glauben, dass Sie Opfer eines Social-Engineering-Angriffs geworden sind, ändern Sie sofort alle Passwörter und überwachen Sie Ihre Konten auf ungewöhnliche Aktivitäten. Informieren Sie das betroffene Unternehmen oder die Organisation.

BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Zero-Day-Angriffe

Zero-Day-Angriffe erfolgen auf unbekannte Sicherheitslücken in Software oder Hardware, bevor der Hersteller die Möglichkeit hat, einen Patch zu erstellen.

ZIEL / SCHADEN

Diese Angriffe können zu schwerwiegenden Datenschutzverletzungen, Systembeschädigungen und Datenverlusten führen.

INFEKTIONSWEG

Durch das Ausnutzen nicht behobener Schwachstellen in Software oder Hardware.

ABWEHR

Halten Sie Ihre Systeme und Software immer auf dem neuesten Stand und verwenden Sie eine mehrschichtige Sicherheitslösung.

BEFREIUNG MÖGLICH?

Ja, durch Patching der betroffenen Software/Hardware und Entfernen der eingedrungenen Malware.

ANGRIFF - WAS NUN?

Wenn Sie glauben, dass Sie Opfer eines Zero-Day-Angriffs geworden sind, aktualisieren Sie Ihre Systeme und Software, führen Sie einen vollständigen Antiviren-Scan durch und informieren Sie Ihre IT-Abteilung.

BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

Malware – Viren, Würmer und Trojaner

Malware ist eine Kategorie von schädlichen Programmen, die Systeme infizieren, beschädigen oder den Zugriff darauf einschränken können. Dazu gehören Viren, Würmer und Trojaner.

ZIEL / SCHADEN

Malware kann dazu führen, dass Systeme langsam laufen, Daten zerstört werden, persönliche oder geschäftliche Informationen gestohlen werden oder dass der Zugriff auf Ihre Systeme und Dateien verwehrt wird.

INFEKTIONSWEG

Oft durch Phishing-E-Mails, infizierte Software-Downloads, Besuch schädlicher Websites oder über infizierte USB-Sticks.

ABWEHR

Installieren Sie eine zuverlässige Antivirensoftware, halten Sie Ihre Systeme und Software auf dem neuesten Stand und seien Sie vorsichtig beim Öffnen von E-Mails und Downloads von unbekannten Quellen.

BEFREIUNG MÖGLICH?

Ja, Antivirensoftware und spezielle Malware-Entfernungsprogramme können oft helfen, Malware zu entfernen und Ihr System wiederherzustellen.

ANGRIFF - WAS NUN?

Führen Sie einen vollständigen Scan mit Ihrer Antivirensoftware durch, isolieren Sie infizierte Systeme, um eine weitere Ausbreitung zu verhindern, und informieren Sie Ihren IT-Support oder einen Sicherheitsexperten.