DELL Technologies

Schnellübersicht: Cybersicherheit

In unserer zunehmend virtuellen Welt nimmt die Cyberkriminalität – wenig überraschend – in alarmierendem Maße zu. **Cyberkriminalität erwirtschaftete im Jahr 2021 rund 6 Billionen US-Dollar** und ist damit nach den Volkswirtschaften der USA und Chinas der drittgrößte Wirtschaftsbereich der Welt.* Die Angreifer gehen dabei von Tag zu Tag intelligenter und raffinierter vor. Wenn Sie jedoch über die neuesten Bedrohungen informiert sind und passende Schutzmaßnahmen ergriffen haben, ist Ihre Onlinesicherheit gewährleistet. **Im Folgenden finden Sie einige der Bedrohungen, die Sie gemeinsam mit Cybersicherheitsexpertinnen von Dell verhindern können, sowie Tipps, wie Sie Ihren Arbeitsplatz und Ihre privaten Geräte schützen können.**

Drive-by-Angriff

Bösartige NutzerInnen erhalten Zugriff auf Ihr System, wenn Sie eine unsichere oder kompromittierte Website besuchen.

Erkennungsmerkmale:

Neue Dateien oder Netzwerkverbindungen auf Ihrem System, die Sie nicht selbst hinzugefügt haben

Unaufgeforderte Anfragen zu Konfigurationsinformationen

TIPP: *Halten Sie Browser und Plug-ins auf dem neuesten Stand*

Ihre Verbindung ist nicht sicher.

Unsichere Hardware

TIPP: *Tätigen Sie Einkäufe nur bei autorisierten Händlern*

Wussten Sie, dass Ihr Drucker gehackt werden kann?

Bedrohungsakteure implementieren Sicherheitslücken direkt in Hardware und Zubehör.

Erkennungsmerkmale:

Angebote, die zu gut sind, um wahr zu sein

Social Engineering

Scammer manipulieren Menschen, indem sie vorgeben, eine juristische Person zu sein oder eine anderweitig autorisierte Rolle innezuhaben, um vertrauliche **personenbezogene oder finanzielle Daten** zu stehlen (auch bekannt als „Phishing"). Der bösartige Code wird über Links oder E-Mail-Anhänge, Direktnachrichten und SMS verschickt.

Erkennungsmerkmale:

Empfang unaufgeforderter E-Mails oder Nachrichten, in denen nach personenbezogenen Daten gefragt wird und die Anweisungen zum Öffnen von Links und Anhängen enthalten

Ungewöhnliche Absender-E-Mail-Adresse, Formulierungen, Rechtschreibung

TIPP: *Behörden melden sich zuerst per Post*

Hier ist doch etwas nicht in Ordnung!

USB-Malware-Angriff

TIPP: *Vorsicht bei unbekannten USB-Laufwerken, auch wenn sie von Freunden stammen*

Hmm … Ist es sicher, dieses USB-Laufwerk anzuschließen?

Kriminelle nutzen Wechseldatenträger wie USB-Laufwerke, tragbare Festplatten, Smartphones, Musikabspielgeräte, SD-Karten und optische Medien (CDs, DVDs, BluRay), um einen Computer oder ein Netzwerk zu infizieren.

Erkennungsmerkmale:

Unerwarteter Zugriff auf Dateien oder neu erstellte Dateien auf dem Gerät

Ausnutzen eines Vertrauensverhältnisses

Ein Hacker nimmt die Rolle einer vertrauenswürdigen Drittpartei ein, wie z. B. einer Arztpraxis, und nutzt deren Ruf, um Patientendaten zu stehlen.

Erkennungsmerkmale:

Ungewöhnliches Anmelde verhalten

TIPP: *Verwenden Sie starke und eindeutige Kennwörter*

Wer sind Sie?

So sorgen Sie für Cybersicherheit

DOs

Verwenden Sie eine Multi-Faktor-Authentifizierung und sichere, eindeutige Kennwörter für alle Konten.

Jedes mit dem Internet verbundene Gerät ist anfällig für Angriffe. Halten Sie Software auf dem neuesten Stand.

Seien Sie wachsam und skeptisch. Lernen Sie, die Taktiken der Scammer zu erkennen.

Teilen Sie Ihre Bedenken mit. Melden Sie der IT-Abteilung mögliche Angriffe und benachrichtigen Sie MitarbeiterInnen, Familie und FreundInnen.

DON'Ts

Werden Sie nicht unachtsam. Halten Sie konsequent alle Sicherheitsvorkehrungen ein.

Klicken Sie nicht auf Links in unerwünschten E-Mails oder Direktnachrichten.

Ignorieren Sie keine Browserwarnungen, wie z. B. „Ihre Verbindung ist nicht sicher" oder „Dies ist keine private Verbindung".

TIPP: *Weitere Informationen unter:* Dell.com/Endpoint-Security

DELL Technologies

*Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics