SOPHOS

Cybersecurity Best Pratices

So bleiben Sie sicher

Um sich vor Cyberangriffen zu schützen, benötigen Sie nicht nur moderne Sicherheitslösungen. Auch mit Ihrem Verhalten können Sie Ihren Schutz maßgeblich beeinflussen. Mit den folgenden Best Practices erhöhen Sie Ihre Sicherheit:

1.	**Installieren Sie Patches frühzeitig und oft** Ungepatchte Schwachstellen waren die Ursache für fast die Hälfte der von Sophos in 2021 untersuchten Cybervorfälle. [1] Je früher Sie patchen, desto weniger Sicherheitslücken können ausgenutzt werden.
2.	**Erstellen Sie regelmäßig Backups und bewahren Sie diese offline und außerhalb des Büros auf** 73 % der von uns befragten IT-Manager konnten bei einem Angriff verschlüsselte Daten mithilfe von Backups wiederherstellen.[2] Verschlüsseln Sie Ihre Backup-Daten und bewahren Sie diese offline und außerhalb des Büros auf. Spielen Sie die Datenwiederherstellung von Backups regelmäßig durch.
3.	**Aktivieren Sie Datei-Erweiterungen** Datei-Erweiterungen werden in Windows standardmäßig ausgeblendet. Bei aktivierten Datei-Erweiterungen können Sie Dateitypen erkennen, die normalerweise nicht an Sie und Ihre Benutzer gesendet werden und deshalb verdächtig sind (z. B. JavaScript-Dateien).
4.	**Öffnen Sie JavaScript (.JS)-Dateien in Notepad** Wenn Sie eine JavaScript-Datei in Notepad öffnen, können keine Schad-Skripte ausgeführt werden und Sie können den Inhalt der Datei gefahrlos überprüfen.

5.

Aktivieren Sie keine Makros in Anhängen, die Sie per E-Mail erhalten

Microsoft hat die automatische Ausführung von Makros schon vor Jahren aus Sicherheitsgründen deaktiviert. Viele Infektionen funktionieren nur, wenn Sie Makros aktivieren. Aktivieren Sie also keine Makros!

6.

Vorsicht bei Anhängen, die Ihnen unaufgefordert zugesendet werden

Cyberkriminelle verlassen sich oft auf ein uraltes Dilemma: Benutzer wissen, dass sie ein Dokument erst öffnen sollten, wenn sie sicher sind, dass es unbedenklich ist. Aber um festzustellen, ob das Dokument unbedenklich ist, müssen sie es öffnen. Lassen Sie im Zweifel lieber die Finger von einem Anhang, der Ihnen verdächtig erscheint.

7.

Überwachen Sie Administrator-Rechte

Überprüfen Sie kontinuierlich die lokalen und Domain-Administrator-Rechte. Behalten Sie im Auge, wer Administrator-Rechte hat, und entziehen Sie die Rechte ggf., wenn sie nicht benötigt werden. Bleiben Sie nicht länger als nötig als Administrator angemeldet.

8.

Regeln Sie den internen und externen Netzwerkzugriff

Lassen Sie Ports nicht geöffnet. Sperren Sie den RDP-Zugriff Ihres Unternehmens und andere Remote-Management-Protokolle. Verwenden Sie außerdem eine Zwei-Faktor-Authentifizierung, und stellen Sie sicher, dass sich Remote-Benutzer bei einem VPN authentifizieren.

9.

Verwenden Sie sichere Passwörter

Über ein schwaches und leicht zu erratendes Passwort können sich Hacker Zugriff auf Ihr gesamtes Netzwerk verschaffen. Nutzen Sie deshalb komplexe Passwörter ohne Bezug auf Ihre Person mit mindestens 12 Zeichen und einer Mischung aus Groß-und Kleinschreibung sowie zufälligen Satzzeichen (Bsp.: Hey527!miTn8?).

1 Active Adversary Playbook 2022 – Sophos
2 Ransomware-Report 2022

2022-09-12 DE (DD)

SOPHOS