Sophos gibt 5 Tipps für Unternehmen am Safer Internet Day

„Cybersicherheit ist kein Ziel, sondern eine Reise“ heißt es in einem Sprichwort. Der Safer Internet Day soll daran erinnern. Es geht heute also weniger darum, speziell heute auf die IT-Sicherheit im Unternehmen – oder auch privat – zu achten, sondern vielmehr diesen Tag zum Anlass zu nehmen, die eigenen Sicherheitsmaßnahmen zu überprüfen.

Sophos beschreibt fünf Maßnahmen, die Unternehmen jeder Größe ergreifen können, um den Cyberkriminellen einen Schritt voraus zu sein.

1. Frühzeitig patchen, oft patchen.
Einen Teil dieser Schlacht hat die gute Seite bereits gewonnen, denn die meisten Unternehmen installieren heutzutage Sicherheitspatches – zumindest irgendwann. Zu viele Organisationen lassen sich immer noch zu viel Zeit und schieben Updates wochen- oder sogar monatelang auf. Die Gegenspieler auf der anderen Seite, die Cyberkriminellen, verlieren dagegen keine Zeit, wenn sie einmal über neue Sicherheitslücken Bescheid wissen. Je länger Unternehmen also mit Updates warten, desto verwundbarer werden sie.

2. Haben Sie alle verwendeten Geräte im Blick.
Egal, ob es im Unternehmen ein so genanntes Bestandsverzeichnis, ein IT-Inventar oder vielleicht auch nur einfach nur eine alte Liste von Computern und Software gibt – Firmen sollten sich einen Überblick verschaffen, was in ihrem Netzwerk vorhanden ist. Das gilt auch für kleine Unternehmen bei denen z.B. alle Mitarbeiter im Home Office arbeiten. Es ist gut, sagen zu können: „Wir haben 10 Laptops und alle wurden von Windows 7 auf Windows 10 aktualisiert.“ Selbst in der Büroecke oder dem Keller `vergessene‘ Computer sollten unter die Lupe genommen werden. Cyberkriminelle suchen gern nach alten, ungepatchten Computern, weil sie wissen, dass sie ein leichtes Sprungbrett für größere Angriffe sein könnten.

3. Richten Sie eine Sicherheitshotline ein.
Es ist ratsam, aufmerksamen Mitarbeitern eine Anlaufstelle zu geben, an der sie die üblichen ersten Vorboten von Cyberkriminalität wie fragwürdige E-Mails, verdächtige Telefonanrufe oder unerwünschte Anhänge melden können. Auf diese Weise installieren Unternehmen ein eigenes Frühwarnsystem, das einen wichtigen Beitrag zur IT-Security leisten kann.
Eine solche Anlaufstelle ist einfach einzurichten, jedes noch so kleine Unternehmen kann dies tun. So muss gar nicht einmal unbedingt eine spezielle Telefonnummer oder sogar ein Callcenter eingerichtet werden – eine leicht zu merkende E-Mail-Adresse wie "cyber911@yourcompany.example" reicht womöglich schon aus.

Ein Hintergrund für diese Maßnahme ist beispielsweise, dass Cyberkriminelle oft beim ersten Versuch zunächst scheitern, weshalb sie in der Regel Phishing-E-Mails an viele verschiedene Empfänger senden oder jede Telefonnummer des Unternehmens anrufen, die sie finden können. Solange, bis jemand einen Fehler macht. Mit einer Sicherheitshotline oder -E-Mail-Adresse wird es bereits der ersten Person ermöglicht, Alarm zu schlagen und damit alle anderen zu schützen.

4. Überdenken Sie Ihre Sicherungsstrategie.
Die meisten Unternehmen wissen heute, dass Backups wichtig sind, und bemühen sich zumindest darum, Zweitkopien von wichtigen Daten aufzubewahren. Aber hier gilt es auch, Vorsicht walten zu lassen, damit keine Zeit mit Backups verschwendet wird, die nicht viel nützen.

Es ist einfach, sich ganz auf Echtzeit-Backups zu verlassen, bei denen Dateien automatisch „live" auf Netzwerkfreigaben oder in die Cloud kopiert werden, wenn sie geändert werden. Cyberkriminelle nehmen sich heute jedoch oft die Zeit, Online-Backups von Unternehmen zu durchsuchen und zu vernichten, bevor sie im Anschluss ihre Angriffe entfesseln.

Es ist daher ratsam, auf eine Sicherheitsstrategie zu setzen, die auch Backups umfasst, die offline und außerhalb des Unternehmens aufbewahrt werden – selbst wenn es sich dabei um etwas Einfaches, wie ein verschlüsseltes, austauschbares Laufwerk handelt, das zu Hause aufbewahrt wird. Backups dienen nicht nur dem Schutz zum Beispiel vor Lösegeldangriffen, es geht dabei auch um die Wiederherstellung von Daten im Notfall, etwa nach Bränden oder Überschwemmungen, die die Geschäftsräume betroffen haben.

5. Die richtigen Passwörter wählen.
Eigentlich scheint dieser Rat mittlerweile überholt, weil jeder Einzelne wie auch jedes Unternehmen inzwischen weiß oder zumindest wissen sollte, wie wichtig gute, sichere Passwörter sind. Wir geben ihn trotzdem noch einmal.

Richtige Passwörter" bedeutet nicht, stets dasselbe Passwort zu verwenden. In einem Unternehmen bedeutet es auch, dass man weiß, wer auf welche Informationen Zugriff haben soll. Es bedeutet zudem, dass man Konten sofort löscht, wenn Mitarbeiter gehen und dass man seine Mitarbeiter dazu ermutigt, die IT-Abteilung oder auch Sicherheitshotline zu informieren (siehe Punkt 3), wenn sie zum Beispiel mit ihrem Passwort Daten sehen können, die sie eigentlich nicht sehen sollten.

Die meisten Unternehmen tun sicher bereits einige, viele oder alle diese Dinge. Dennoch ist der Safer Internet Day ein guter Anlass, die eigene Strategie zur Cybersicherheit am Arbeitsplatz noch einmal zu prüfen.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de