Fachjargon

Sicherheitsbegriffe einfach erklärt

SHARP

Be Original.

geschützte Geräte

Seien Sie stets wachsam!

Cyberkriminalität birgt diverse Risiken für digital vernetzte Unternehmen

Das Verständnis dafür, wie Angriffe aussehen, wie sie zustande kommen und welche Auswirkungen sie auf Ihr Unternehmen haben können, sollte nicht unterschätzt werden.

Für viele kleine und mittlere Unternehmen (KMU) ist die eigentliche Bekämpfung der Bedrohung jedoch nicht der erste Ansatzpunkt. Um einen wirklichen Schutz vor Cyber-Bedrohungen zu gewährleisten, müssen Sie das Dickicht aus Fachbegriffen entwirren – und verstehen.

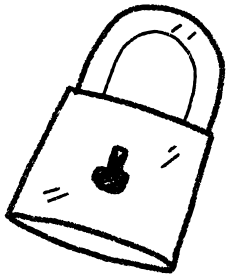
Um Sie dabei zu unterstützen, haben wir einige wichtige Begriffe herausgesucht, und gehen hier näher darauf ein.

Netzwerksicherheit

Das stählerne Vorhängeschloss, das Ihre Informationen schützt

Ähnlich, wie Sie Ihre wertvollsten Dinge in einem Safe aufbewahren oder Ihr Fahrrad mit einem Schloss sichern, schützt die Netzwerksicherheit die sensiblen Daten Ihres Unternehmens.

In jedem Unternehmensnetzwerk sollte Ihr Sicherheitsschutz ein Intrusion Detection System (IDS) umfassen, das potenzielle Bedrohungen, verdächtige Aktivitäten und unbefugte Zugriffsversuche auf digital verbundene Geräte wie Laptops und Drucker überwacht und identifiziert.



Datenschutzverletzung

Kann mit dem Diebstahl Ihres Portemonnaies im Zug verglichen werden

In vielen Fällen wissen Sie überhaupt nicht, dass Sie bestohlen wurden, bis sich die Daten bereits in den falschen Händen befinden. Eine Datenschutzverletzung liegt dann vor, wenn sensible Daten, ganz gleich ob sie einem Unternehmen oder einem Kunden gehören, von böswilligen Akteuren (Cyberkriminellen) gestohlen werden.

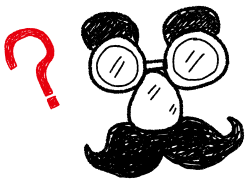
Dies kann geschehen, ohne dass es das Unternehmen merkt oder den Zugriff autorisiert hat. Eine Datenschutzverletzung kann letztendlich zu einem Vertrauensverlust bei Kunden oder Benutzern, einem beschädigten Ruf der Marke und sogar zu kostspieligen Geldstrafen führen. Für die Bestohlenen.

Phishing, Smishing und Vishing

Diese Begriffe bezeichnen Situationen, in denen sich Hacker als Ihr Chef, Kunde oder bester Freund ausgeben

Diese Arten von Angriffen sind nicht immer offensichtlich, aber sie sind weit verbreitet. Tatsächlich beginnen etwa 90 % der Cyberangriffe mit Phishing (via E-Mail), wobei die Zahl der Smishing- (SMS) und Vishing-Angriffe (Sprachanrufe) ebenfalls zunimmt. Wir alle kennen diese verräterisch aussehenden E-Mails, die bestenfalls in unserem Spam-Ordner landen.

Phishing, Smishing und Vishing sind Cyberangriffe, die die Benutzenden dazu verleiten, auf E-Mails zu klicken, auf Nachrichten zu antworten oder Anrufe anzunehmen, die sie für legitim und sicher halten. Wenn sich der Angriff als erfolgreich erweist, werden Mitarbeitende unwissentlich dazu verleitet, sensible Daten, wie ihr Netzwerkpasswort, preiszugeben.



Malware

Schädliche Software, die mit schlechten Absichten programmiert wird

„Malware“ steht für Malicious Software (schädliche Software). Dabei handelt es sich um Software, die von Cyberkriminellen entwickelt wurde, um den Netzwerksystemen Ihres Unternehmens Schaden zuzufügen und Sie an Ihrer Nutzung zu hindern. Wenn Sie eine Phishing-E-Mail öffnen, auf einen verdächtigen Link klicken oder eine Website aufrufen, die bereits kompromittiert wurde, kann Malware in Ihr System eindringen.

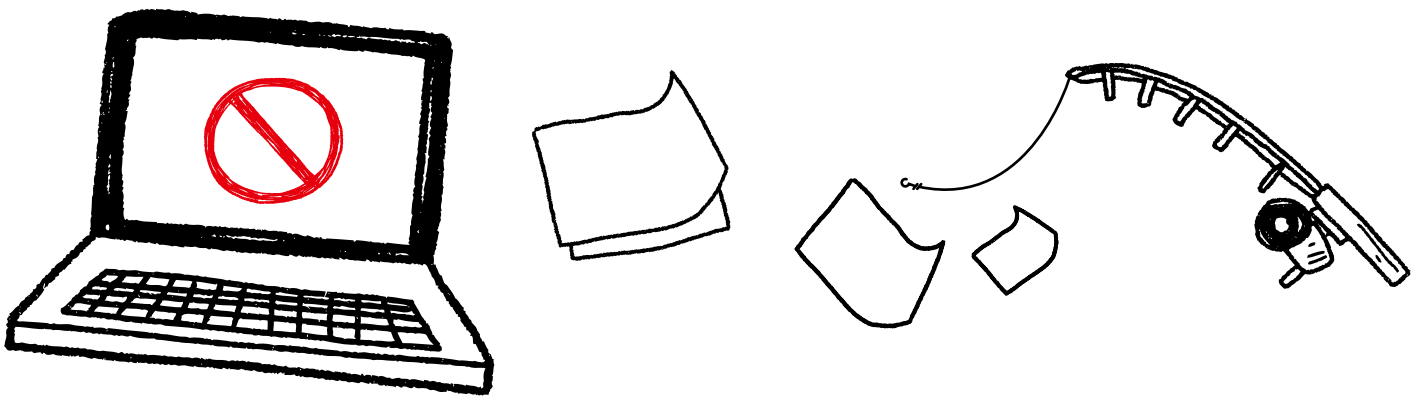
Sobald dies geschehen ist, können die in Ihrem Netzwerk gespeicherten Daten für Hacker zugänglich sein, was zu einer Ausweitung des Angriffs führen kann.

Ransomware

Ihre Daten werden als „Geisel“ genommen

Ransomware ist eine Form von Malware, die von Cyberkriminellen eingesetzt wird, um den Zugriff auf wichtige Geschäftsdaten zu verweigern, indem sie diese verschlüsselt (in Code umwandelt). Jede Art von digital vernetztem Unternehmen besitzt Daten – von Finanzunterlagen, über Patientendaten, bis hin zu vertraulichen juristischen Dokumenten. Der uneingeschränkte Zugang zu diesen Daten ist für den Betrieb eines Unternehmens von entscheidender Bedeutung.

Gelingt es Ransomware, in Ihr Netzwerk einzudringen, kann Ihr Unternehmen diesen Zugang jedoch verlieren. Um ihn zurückzuerlangen, müssen oft hohe Geldsummen (Lösegelder) an die Hacker, die den Angriff durchgeführt haben, gezahlt werden.



Endpunktsicherheit

Stellen Sie sicher, dass all Ihre Geräte genauso sicher sind wie Ihr Schreibtisch

Ihre digitale Verteidigung beginnt und endet nicht mit Ihrem Schreibtisch. Die Endpunktsicherheit („End-point security“) bezieht sich auf den Prozess, der sicherstellt, dass all Ihre „Endpunkte“ – von Tablets über Smartphones bis hin zu anderen, mit dem Internet verbundenen Geräten wie Ihrem Bürodrucker – über einen einheitlichen Schutz verfügen. Dieser Schutz sollte zentral verwaltet und überwacht werden, um einen aussagekräftigen Überblick über Ihre Cybersicherheit zu erhalten.

Patch-Management

Aktualisieren Sie Ihr Smartphone stets auf die neueste Version Ihres Betriebssystems

Wir kennen diese vermeintlich nervigen Meldungen zu Software-Updates auf unseren Smartphones: „Jetzt auf Windows 10 aktualisieren“ oder „iOS 9.999 installieren“. Diese Updates sind jedoch eine wichtige Sicherheitsmaßnahme.

Das Patch-Management spielt Updates für Software, Treiber und Firmware auf, um Sicherheitslücken in Ihrem Netzwerk zu schließen. Dazu gehört auch die Überwachung der Compliance, die Verwaltung der Anwendungen, die Ihr Unternehmen nutzt, und die Sicherstellung, dass Ihre Systeme ihr volles Potenzial ausschöpfen.

Verschlüsselung

Stellen Sie sich vor, all Ihre Daten befinden sich in einer Tombola-Kugel

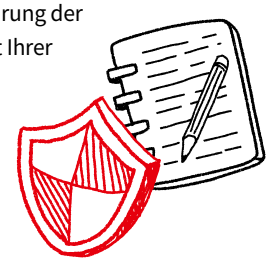
Wie können Sie verhindern, dass jemand eine vertrauliche Nachricht liest? Indem Sie die Wörter, Buchstaben und Zahlen wild durcheinander mischen. Im Wesentlichen ist das Verschlüsselung. Der „Klartext“ Ihrer sensiblen Daten wird in einen „Chiffretext“ umgewandelt, der diese Daten für jeden, der keinen „kryptographischen Schlüssel“ hat, z. B. den Code, den Sie für den Zugang zu einem gesicherten drahtlosen Netzwerk verwenden, unlesbar macht. In einem Unternehmen sollte die Verschlüsselung auf alle Geräte angewendet werden, z. B. auf Ihr Smartphone und Ihren Laptop, damit die darauf gespeicherten Inhalte auch dann nicht gelesen werden können, wenn das Gerät verloren geht oder gestohlen wird.

Krisenreaktion

Ihr Aktionsplan zur Abwehr eines Cyberangriffs

Und was ist die erste Anlaufstelle, wenn Ihr Unternehmen von einem Cyberangriff betroffen ist? Die Krisenreaktion („Incident response“, IR) ist der systematische Ansatz eines Unternehmens, das planen will, wie es auf Cybersicherheitsbedrohungen reagiert und diese effektiv bewältigt.

Ohne einen soliden Krisenreaktionsplan – für den Fall, dass Sie durch einen Angriff bedroht werden – wird Ihr Unternehmen nicht in der Lage sein, einen solchen Angriff abzuwehren. Die Krisenreaktion ist damit entscheidend für die Wahrung der Integrität, Vertraulichkeit und Verfügbarkeit Ihrer sensiblen Geschäftsdaten.



Wir haben Ihnen nichts Neues erzählt? Gut so. Dann haben Sie sich wohl bereits intensiv mit dem Thema Cybersicherheit auseinandergesetzt. Womöglich haben wir Ihnen aber auch die Augen geöffnet und Sie wissen jetzt, dass der Schutz vor Cyber-Bedrohungen für jedes digital vernetzte Unternehmen von höchster Wichtigkeit ist. Für Ihres auch? Sicher sein, sicher bleiben.

Sharp Electronics Europe GmbH,
Zweigniederlassung Österreich
Handelskai 342, A-1020 Wien
Tel.: +43 1 727 19-0
www.sharp.at

SHARP
Be Original.