Die 10 wichtigsten Tipps

zum Schutz Ihres kleinen oder mittelständischen Unternehmens

Ein Unternehmen vor den neuesten Internetbedrohungen zu schützen, ist zu einer äußerst komplizierten Angelegenheit geworden. Die Folgen externer Angriffe, interner Sicherheitsverletzungen und die missbräuchliche Nutzung des Internets haben die Sicherheit zu einem Topthema auf der Tagesordnung von kleinen Unternehmen gemacht. Was also sollten Sie über Sicherheit wissen, und welche wichtigen Elemente gilt es dabei zu beachten? Im Folgenden beleuchtet Trend Micro dieses komplexe Thema.

1 MALWARE MUSS DRAUSSEN BLEIBEN

Ebenso, wie Sie vermutlich nicht im Traum daran denken würden, Ihre Haustür nachts unverschlossen zu lassen, würden Sie Cyberkriminelle nie in Ihr Unternehmen einladen. Aber wenn Sie Ihre Computer nicht schützen, beispielsweise indem Sie keine entsprechende Firewall und Antivirensoftware einsetzen, tun Sie genau das.

Tatsächlich hat der Zahlungsdienstleister NACHA – The Electronic Payments Association eine Warnung veröffentlicht, nach der es immer mehr Angriffe auf kleine Unternehmen gibt. *ComputerWorld* berichtete, „laut der Warnung von NACHA haben es Cyberkriminelle offensichtlich auf kleine Unternehmen abgesehen, da diese häufig keine starken Authentifizierungsmaßnahmen, Transaktionskontrollen und entsprechenden Berichterstellungsfunktionen einsetzen. In einigen Fällen, so die Warnung, versuchen die Angreifer, Mitarbeiter von Kleinunternehmen auf Phishing-Websites umzuleiten, die der Website des Finanzinstituts, bei dem ihr Unternehmen Kunde ist, täuschend ähnlich sehen. Dort sollen sich die ahnungslosen Mitarbeiter dann mit ihren Zugangsdaten anmelden."

Malware ist bösartige Software, die in PCs und Netzwerke eindringt oder diese beschädigt, und zwar ohne Ihr Wissen und Ihre Zustimmung.

- **Nutzen Sie die Firewall.** Ein guter Internetrouter hat eine integrierte Firewall (die Sie in jedem Fall aktivieren sollten), aber angesichts der heutigen komplexen Malware reicht diese Firewall nicht aus.
- **Schützen Sie die PCs.** Die ideale Sicherheitssoftware geht über Standardschutzmaßnahmen hinaus und befindet sich auf dem PC, ohne die Leistung des PCs, Laptops oder Netzwerks einzuschränken. Der ideale Schutz wehrt Identitätsdiebstahl, gefährliche Websites und Hacker-Angriffe ab. Und zwar in einer einzigen Lösung.
- **Sehen und abwehren.** Entscheiden Sie sich für eine Lösung, bei der Sie über eine zentrale Konsole sowohl mobile Anwender als auch sämtliche PCs und Server im Auge behalten können.
- **Mobile Anwender ganz leicht überwachen.** Gute Sicherheitslösungen verfügen über Location Awareness. Diese Funktion passt die Sicherheitseinstellungen auf Laptops automatisch an die beste Schutzstufe an, während sich die Mitarbeiter frei inner- oder außerhalb des Büros bewegen.
- **E-Mail-Verkehr filtern.** Spam-Schutz reduziert unerwünschte E-Mails und wehrt Risiken und Störungen für die Mitarbeiter ab. Stoppen Sie Spam, ehe er Ihr Unternehmen erreicht!

2 VERFASSEN SIE RICHTLINIEN

Sie glauben, Ihr Unternehmen sei Hackern eine Nummer zu klein? Sind Sie sicher? Größe spielt keine Rolle, wenn es um Onlinekriminalität und -betrug geht, und kleine Unternehmen sind leichte Beute, da ihre IT-Ressourcen häufig überlastet sind. Darum ist es wichtig, dass Ihr Unternehmen Sicherheit ernst nimmt: Schulen Sie Ihre Mitarbeiter immer wieder über Ihre Sicherheitsanforderungen. Schreiben Sie sie nieder. Kommunizieren Sie sie an Ihre Mitarbeiter. Setzen Sie sie durch.

Ihre Richtlinien sollten unter anderem Folgendes beinhalten:

- **Teilen Sie mit, was in Ordnung ist und was nicht.** Welche Anwendungen dürfen auf die Unternehmenscomputer geladen werden, welche nicht?
- **Verlangen Sie sichere Kennwörter.** Weitere Informationen finden Sie unter Tipp 4.
- **Seien Sie konsequent.** Was geschieht, wenn die Richtlinien nicht eingehalten werden? Lassen Sie auf Worte auch Taten folgen.
- **Nutzen statt missbrauchen.** Wie sieht die angemessene Nutzung eines Unternehmenscomputers aus? Zweifellos gehört die Nutzung des Internets dazu.
- **Klären Sie Mitarbeiter über E-Mails auf.** Sprechen Sie dabei über interne und externe Kommunikation und darüber, was geöffnet oder weitergeleitet werden sollte und was nicht.
- **Verschlüsseln oder nicht verschlüsseln?** Legen Sie fest, ob Ihre sensiblen Daten durch eine E-Mail-Verschlüsselungslösung geschützt werden sollen und wann.
- **Schaffen Sie eine Anlaufstelle.** An wen können sich Mitarbeiter wenden, wenn sie allgemeine Fragen zu Richtlinien oder Computersicherheit haben?

3 GEHEN SIE SOZIALE MEDIEN AN, BEVOR DIESE ZUM PROBLEM WERDEN

Ein Ende der sozialen Netzwerke ist nicht in Sicht, also geben Sie Ihren Mitarbeitern Best Practices und Leitfäden an die Hand. Im Folgenden stellen wir Ihnen Möglichkeiten vor, um Risiken in sozialen Netzwerken zu senken:

- **Guck mal, wer da spricht.** Bestimmen Sie, wer im Namen des Unternehmens kommunizieren darf, und erlauben Sie nur diesen Mitarbeitern, über interne und externe Ereignisse zu berichten.
- **Bestimmen Sie, was vertraulich ist.** Decken Sie in Ihren Sicherheitsrichtlinien soziale Netzwerke, wie Facebook, Twitter, LinkedIn usw., mit Ihrer Geheimhaltungsverpflichtung ab.

- **Erstellen Sie Leitfäden und ein Forum, um diese zu entwickeln.** Das Bloggen und Posten in sozialen Netzwerken im Namen des Unternehmens sollte Leitfäden unterliegen, die regeln, welche Informationen veröffentlicht werden dürfen und von wem. Leitfäden müssen über die Sicherheit hinausgehen:
  - Blogger sollten sich selbst als Mitarbeiter bzw. als vom Unternehmen Beauftragte zu erkennen geben. Andernfalls müssen Sie mit Gegenreaktionen rechnen.
  - Bestimmen Sie den Tonfall des Blogs.
  - Schützen Sie Daten und Persönlichkeit von Kunden. Erinnern Sie Kunden daran, keine persönlichen Daten zu posten. Bieten Sie Ihnen eine Kontaktmöglichkeit bei Fragen zu vertraulichen Informationen.
  - Bestimmen Sie, wann Support-Informationen in sozialen Netzwerken veröffentlicht werden sollten.
  - Holen Sie sich Unterstützung durch die Führungsebene/den Geschäftsinhaber, damit Leitfäden schnell und unter Beachtung der Unternehmensanforderungen angepasst werden können.
  - Greifen Sie auf andere Quellen wie BlogWell (www.blogwell.com) zurück, um Ihre Leitfäden zu entwickeln und mehr über soziale Netzwerke zu erfahren.
- **Öffnen Sie sich sozialen Netzwerken, aber seien Sie clever.**
  - Sie sollten nur Informationen veröffentlichen, die Sie – je nach Zweck – ohne Bedenken einer breiten Öffentlichkeit bereitstellen möchten.
  - Gehen Sie vom Schlimmsten aus, um die besten Ergebnisse zu erzielen. Fordern Sie Ihre Mitarbeiter auf, die Menge der persönlichen Daten, die sie online freigeben, einzuschränken – zu ihrem eigenen Schutz und dem Ihres Unternehmens.
  - Nehmen Sie nur Personen in Ihre Kontaktliste auf, denen Sie vertrauen.
  - Klicken Sie möglichst nicht auf unerwartete Links von unbekannten Absendern.
  - Vertrauen Sie niemals Personen, die Sie nicht gut kennen.

4 SCHÜTZEN SIE SICH MIT KENNWÖRTERN

Ob es Ihnen gefällt oder nicht: Kennwörter sind der Schlüssel zu den Netzwerken der meisten Kleinunternehmen. Darum sind sie für den Schutz Ihrer Netzwerke unerlässlich. Man braucht kein Statistikgenie zu sein, um zu begreifen, dass Kennwörter umso sicherer sind, je mehr Zeichen sie enthalten.

- **Fangen Sie stark an.** Verlangen Sie sichere Kennwörter mit mindestens 8 Zeichen einschließlich Zahlen, damit Sie einfache Angriffe, die Kennwörter „erraten", abwehren können.
- **Zeit für Veränderung.** Begrenzen Sie die Gültigkeit von Kennwörtern, und fordern Sie die Anwender auf, Kennwörter regelmäßig zu ändern.
- **Sicherheitsbewusstsein.** Verdeutlichen Sie Ihren Mitarbeitern, dass das Niederschreiben von Kennwörtern, das Speichern auf Mobiltelefonen oder die Verwendung von leicht zu erratenden Kennwörtern eine echte Gefahr für das Unternehmen darstellt.
- **Kombinieren Sie.** Verwenden Sie für die sichersten Kennwörter keine Wörter. Nutzen Sie stattdessen zufällige Buchstaben, Zahlen und Sonderzeichen. Behelfen Sie sich notfalls mit Tastaturmustern: qWe4%6zUi ist ein viel sichereres Kennwort als golrish#3.

5 NEHMEN SIE INTERNETSICHERHEIT ERNST

Das Internet eignet sich hervorragend, um Geschäftsabläufe zu fördern. Aber es kann auch zu einem erhöhten Malware-Aufkommen führen, wenn Ihre Unternehmenssicherheit keine proaktive Content-Überprüfung zur Ermittlung von Malware anbietet und Sie bei möglichen Problemen nicht warnt. Wählen Sie eine Sicherheitslösung, mit der Sie die neuesten Bedrohungen abwehren und Ablenkungen Ihrer Mitarbeiter minimieren:

- **Stoppen Sie bösartige Links.** Verlassen Sie sich nicht darauf, dass sich Ihre Mitarbeiter Gedanken über die Sicherheit machen oder ihren Internet- oder Netzwerkzugriff einschränken. Automatisieren Sie Updates, und machen Sie die Sicherheit für Ihre Mitarbeiter transparent.
- **Wahren Sie die Produktivität des Internets.** Neben entsprechenden Leitfäden sollten Sie Lösungen auswählen, die eine unangemessene Internetnutzung unterbinden. URL-Filter können den Zugriff auf nicht produktive Websites vollständig oder auf die Geschäftszeiten begrenzt sperren. Und mit Lösungen zum Schutz vor gefährlichen Links bleiben Ihr Unternehmen, Ihre Mitarbeiter und Ihre Daten in Ihrer Hand und nicht in der von Identitäts- oder Datendieben.

6 BINDEN SIE IHRE MITARBEITER EIN

Wir alle wissen, für welche Schlagzeilen ein Datenverlust sorgen kann. Aber wussten Sie, dass bis zu 80 % aller Datenverluste auf menschlichem Fehlverhalten beruhen, indem vertrauliche Daten entweder an die falschen Personen oder auf dem falschen – nämlich nicht ausreichend geschützten – Weg versendet werden?

- **Richtlinien einhalten oder den Laden dichtmachen.** Naja, Dichtmachen ist vielleicht übertrieben. Aber angesichts der wachsenden Auflagen werden sich die Konsequenzen, die sich aus Datenverlust und versehentlichen Datenlecks ergeben, noch verstärken. Schulen Sie also Ihre Mitarbeiter zu den regulatorischen Anforderungen und Best Practices zum Schutz von Daten. Erklären Sie ihnen, welche Risiken ein Nichteinhalten der Regeln mit sich bringt. Machen Sie ihnen klar, dass sie verantwortlich dafür sind, Risiken zu senken.
- **Erklären Sie Ihren Mitarbeitern, warum ihre Mithilfe so wichtig ist.** Wenn die einzelnen Mitarbeiter keine Virensuchläufe ausführen, oder wenn Sie unangemessene Materialien versenden, drohen dem Unternehmen Malware-Angriffe, Gerichtsverfahren und Rufschädigung.
- **Werden Sie vertraulich.** Klären Sie Ihre Mitarbeiter darüber auf, welche Arten von Daten vertraulich sind und welche möglichen Probleme entstehen können, wenn diese Dokumente oder Dateien nach außen gelangen.

7 PROFITIEREN SIE VON IHRER BEZIEHUNG ZU IHREM FACHHÄNDLER/BERATER

Eine gute Beziehung mit Ihrem IT-Fachhändler/-Berater bedeutet, dass Sie immer einen vertrauenswürdigen Berater zur Seite haben, an den Sie sich wenden können, wenn es um IT-Probleme geht.

- **Fordern Sie mehr.** Anstatt Ihnen nur den besten Preis oder besondere Verkaufsaktionen anzubieten, sollte der Fachhändler oder IT-Berater in der Lage sein, Sie ganz unabhängig zu Ihrer IT-Infrastruktur zu beraten. Er kann und sollte Ihnen bei der Wahl der richtigen Lösung für Ihr Unternehmen helfen, die mit Ihren Anforderungen wächst und Ihre IT-Investitionen schützt. Tut der Fachhändler das nicht, dann wechseln Sie.
- **Lagern Sie die Verwaltung aus.** Ihr IT-Fachhändler oder -Berater bietet möglicherweise sogar an, die Sicherheitslösung für Sie zu verwalten. Das bedeutet für Sie: weniger Aufwand und noch besserer Schutz.

8 MIT GUTEM BEISPIEL VORAN

Wenn Sie den Weg nicht gehen, dann wird Ihnen auch keiner folgen. Egal, ob Sie eine führende Position einnehmen oder nicht – Menschen schauen sich um, um zu sehen, was die anderen tun. Es bedarf also nur einer Person, um etwas zu bewegen.

- **Seien Sie ein gutes Beispiel.** Schon eine Person genügt, um einen hartnäckigen Virus im Unternehmen zu verbreiten. Das sollten nicht Sie sein.
- **Seien Sie Vorreiter.** Wenn Sie eine bessere Schutzmethode gefunden haben oder von einer neuen Bedrohung hören, lassen Sie es die anderen wissen. Sprechen Sie sich mit anderen Abteilungen über Best Practices ab.

9 BLEIBEN SIE AUF DEM LAUFENDEN

Stellen Sie sicher, dass Ihre mobilen Anwender, PCs und Server den besten verfügbaren Bedrohungsschutz einsetzen. Manuelle oder unregelmäßige Sicherheitsupdates öffnen Bedrohungen Tür und Tor. Am Klischee ist etwas dran: Man ist nur so sicher wie das letzte Update.

- **Entlasten Sie die PCs.** Ihre Sicherheitslösung verlangsamt Ihre PCs? Da sind Sie nicht alleine. Bei herkömmlichen Sicherheitslösungen hört man diese Klage häufig. Halten Sie nach Lösungen Ausschau, bei denen das Rechenzentrum des Anbieters die Arbeit mithilfe von Hosting-Funktionen erledigt. Ihre PCs und Server sollten Ihre Geschäftsdaten verarbeiten, statt primär mit den Sicherheitsanforderungen belastet zu sein.
- **Verlassen Sie sich nicht auf alte Antiviren-Lösungen.** Herkömmliche Virenschutzlösungen filterten Bedrohungen bisher durch Abgleich der Dateien mit ihrem jeweiligen Fingerabdruck oder ihrer Signaturdatei auf jedem Computer. Aktuelle Bedrohungen aber vermehren sich exponentiell – seit 2004 um über 2.000 %. Das Versenden von mehr Signaturdateien führt also unweigerlich zu einer Überlastung Ihrer Computer. Neue Erkennungsmethoden arbeiten im Hintergrund. Dort überprüfen sie die Absender von E-Mails sowie Dateien und Websites, um Sie noch besser und schneller zu schützen, ohne Ihre PCs zu verlangsamen.
- **Automatisieren Sie Updates für Betriebssysteme.** Vereinfachen Sie die Verteilung von Patches auf PCs so weit wie möglich. Die Sicherheitslücken in Ihrem Betriebssystem sind die Hauptangriffsstelle für Bedrohungen. Stellen Sie also sicher, dass diese Patches schnell und automatisch verteilt werden.
- **Fordern und überprüfen Sie die Einhaltung von Patch-Installationen.** Stellen Sie Ihren Anwendern Informationen über erforderliche Softwareversionen zur Verfügung und darüber, wie sie überprüfen können, welche Version auf ihrem PC installiert ist. Geben Sie ihnen Links und Anweisungen zur Aktualisierung auf die korrekte Version an die Hand. Wenn die Anwender sehen, dass Sie die Einhaltung ernst nehmen, befolgen sie die Richtlinien eher.

10 ENTSCHEIDEN SIE SICH FÜR EINEN SICHERHEITSPARTNER UND KEINEN BLOSSEN ANBIETER

Wählen Sie einen Partner, der die einzigartigen Sicherheitsanforderungen in kleinen Unternehmen versteht.

- **Wählen Sie einen fokussierten Sicherheitsanbieter.** Prüfen Sie, ob Sicherheit zum Kerngeschäft des Anbieters gehört oder nur einen Teil des Unternehmens ausmacht.
- **Prüfen Sie die Erfahrung des Anbieters.** Anbieter, die jahrelange Erfahrung mit dem Schutz vor diversen Bedrohungen und Expertise im Bereich Klein- und Großunternehmen haben, können Sie in Sachen Sicherheit am besten unterstützen.

WEITERFÜHRENDE INFORMATIONEN

- TrendWatch bietet Schulungsvideos, Whitepaper und mehr: www.trendmicro.de/sicherheitsinformationen
- www.trendmicro.de/kleinunternehmen bietet Videos und Informationen zu Trend Micro Produkten, die speziell für kleine Unternehmen entwickelt wurden.

GEHEN SIE EINEN SCHRITT WEITER

Anhand der folgenden Checkliste können Sie überprüfen, ob Ihr Unternehmen im Kampf gegen Sicherheitsbedrohungen gut aufgestellt ist. Anschließend können Sie die nächsten Schritte festlegen.

TIPP	DURCHGEFÜHRTE MASSNAHMEN
1. Malware muss draußen bleiben	☐ Installieren und verwenden Sie eine Sicherheitslösung, die vor diversen Bedrohungen schützt, wie Viren, Internet-Bedrohungen, Spyware, Bots usw. ☐ Wählen Sie eine Lösung, die lokale und Remote-PCs und Server überwachen und verwalten kann. ☐ Behalten Sie im Auge, was geschützt ist, indem Sie eine Lösung mit einer zentralen Konsole für Remote-Anwender, interne PCs, File- und Mailserver wählen. ☐ Überwachen Sie mobile Anwender ganz leicht, indem Sie eine Lösung mit Location Awareness einsetzen. ☐ Verwenden Sie einen Spam-Schutz zum Filtern des E-Mail-Verkehrs.
2. Verfassen Sie Richtlinien	☐ Schreiben Sie Ihre Richtlinien unbedingt nieder! ☐ Schulen Sie Ihre Mitarbeiter, und behandeln Sie die IT-Sicherheitsrichtlinien wie einen Vertrag. ☐ Ergreifen Sie bei Richtlinienverstoß Maßnahmen. ☐ Legen Sie fest, was Mitarbeiter auf Unternehmenscomputern tun dürfen, und was nicht. ☐ Schulen Sie Mitarbeiter zu Best Practices für E-Mails, um Phishing und Spam zu vermeiden. ☐ Verschlüsseln Sie E-Mails, wenn deren Inhalt geschützt werden soll. ☐ Ernennen Sie eine Anlaufstelle oder einen Hauptkontakt für Fragen zur IT-Sicherheit.
3. Gehen Sie soziale Netzwerke an	☐ Bestimmen Sie, wer Blog-Beiträge zum Unternehmen verfassen und veröffentlichen darf. ☐ Legen Sie fest, was vertraulich ist, und was nicht. ☐ Erstellen Sie Leitfäden und ein Forum, um diese zu entwickeln. ☐ Öffnen Sie sich sozialen Netzwerken, aber gehen Sie geschickt mit Informationen um, die Mitarbeiter veröffentlichen.
4. Beginnen Sie mit Kennwörtern	☐ Verlangen Sie sichere Kennwörter. ☐ Legen Sie Zeitbeschränkungen für Kennwörter fest. ☐ Schützen Sie Kennwörter – sie sollten nicht notiert oder auf dem Smartphone gespeichert werden. ☐ Kombinieren Sie Buchstaben und Ziffern, um Datendiebstahl zu verhindern.
5. Nehmen Sie Internetsicherheit ernst	☐ Der Standort ist entscheidend. Schützen Sie Ihre mobilen Mitarbeiter also mit Location-Awareness-Lösungen. ☐ Nutzen Sie automatische Schutzfunktionen, um gefährliche Weblinks und nicht produktive Websites zu sperren.
6. Lassen Sie sich von Ihren Mitarbeitern helfen	☐ Befolgen Sie behördliche Auflagen und bewährte Sicherheitsverfahren. ☐ Erklären Sie Ihren Mitarbeitern, weshalb sie einen entscheidenden Beitrag zur Sicherheit leisten. ☐ Setzen Sie Sicherheitsrichtlinien durch. ☐ Unterstreichen Sie immer wieder, was vertraulich ist.
7. Holen Sie sich einen Fachhändler/Berater an Bord	☐ Fordern Sie mehr als bloße Auftragserledigung – suchen Sie einen Partner, der Ihnen auch als zuverlässiger Berater zur Seite steht. ☐ Lagern Sie die Sicherheitsverwaltung an Ihren IT-Fachhändler oder -Berater aus, und sparen Sie wertvolle Zeit und Energie für Ihr Unternehmen.
8. Mit gutem Beispiel voran	☐ Ein Vorbild sollte sich entsprechend verhalten. Handeln Sie also gemäß den Richtlinien. ☐ Suchen Sie eine zuverlässige Quelle für Sicherheitsinformationen, und nutzen Sie diese regelmäßig.
9. Bleiben Sie auf dem Laufenden	☐ Entlasten Sie Ihren PC, indem Sie eine Lösung mit zentral gehosteter Datenverarbeitung auswählen. ☐ Verlassen Sie sich nicht auf Ihren alten Virenschutz – setzen Sie mehrere Erkennungsprozesse ein. ☐ Automatisieren Sie Updates für Betriebssysteme. ☐ Fordern und überprüfen Sie die Einhaltung von Patch-Installationen.
10. Suchen Sie sich einen Sicherheitspartner	☐ Entscheiden Sie sich für einen Anbieter mit klarem Fokus auf Sicherheit. ☐ Überprüfen Sie die Kompetenz des Anbieters. Suchen Sie sich ein etabliertes Unternehmen mit Erfahrung im Bereich Groß- und Kleinunternehmen.

Weitere Informationen erhalten Sie bei Ihrem Trend Micro Fachhändler oder unter: www.trendmicro.de/kleinunternehmen.

TREND MICRO™

www.trendmicro.com