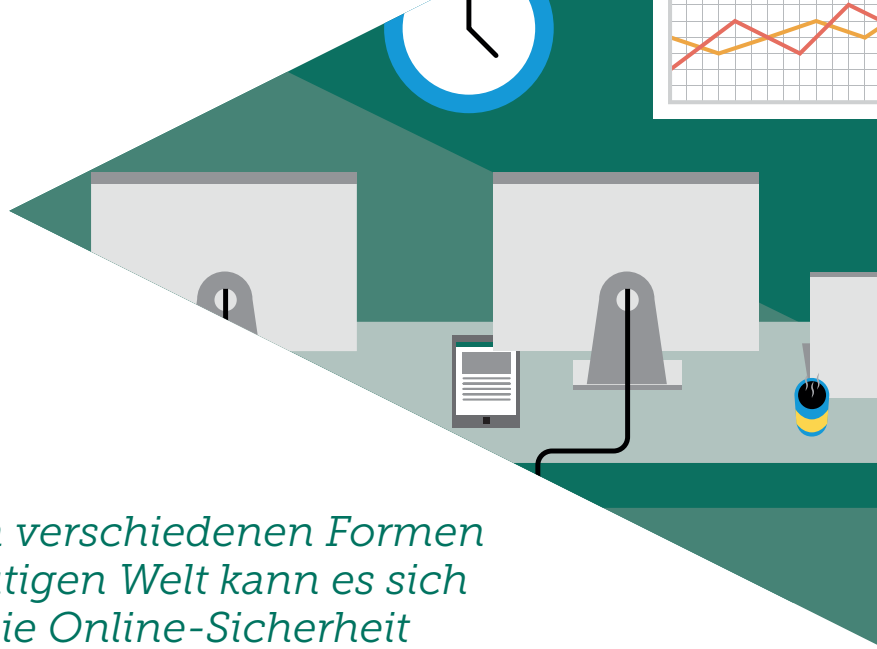
PRAKTISCHER LEITFADEN ZUM IT-SICHERHEITSVERFAHREN FÜR KLEINUNTERNEHMEN

Umfassende IT-Sicherheit für Ihr Unternehmen gewährleisten

#protectmybiz

KASPERSKY lab



Kleinunternehmen gibt es in verschiedenen Formen und Größen. Aber in der heutigen Welt kann es sich kein Unternehmen leisten, die Online-Sicherheit außen vor zu lassen – egal, ob Sie ein Team haben, das in einem Büro arbeitet, oder als Einzelner von zu Hause aus tätig sind. Dieses Thema betrifft jeden.

Obwohl Cyberverbrechen häufig in den Schlagzeichen sind, erregen meist nur Angriffe auf „Multis" oder Regierungen echte Aufmerksamkeit. Wobei die Angriffe auf kleinere Unternehmen ebenso ernstzunehmen sind.

Allein im Jahr 2014 wurden 143 Millionen neuer Malware-Objekte entdeckt.[1] Die Mehrheit davon war gegen Einzelpersonen und Unternehmen gerichtet, die sich selbst nicht als potentielle Opfer einschätzen würden.

Tatsächlich ist jeder ein potentielles Ziel. Die positive Nachricht: es besteht ein großer Unterschied zwischen einem «potentiellen Ziel» und einem «tatsächlichen Opfer».

Entscheidend ist, auf mögliche Angriffe vorbereitet und bestmöglich geschützt zu sein. Aus diesem Grund haben wir den vorliegenden Leitfaden zusammengestellt: Wir möchten Ihnen das nötige Know-how an die Hand geben, um Ihr Unternehmen zu schützen.

? WAS IST MALWARE?

Der Begriff „Malware" bezieht sich auf Computerprogramme, die in böswilliger Absicht entwickelt wurden. Diese Programme greifen normalerweise Geräte an, ohne dass der Benutzer etwas davon mitbekommt. Kaspersky Lab gehört zu den weltweit führenden Unternehmen in der Erkennung und Bekämpfung von Malware.

? WARUM BENÖTIGE ICH SCHUTZ?

Cyberkriminelle müssen nicht Ihr Bankkonto leerräumen, um Ihrem Unternehmen finanziellen Schaden zuzufügen. Störungen aufgrund von Malware können Produktivität und Cashflow beeinträchtigen und so eine Reihe unerwünschter Auswirkungen nach sich ziehen. Sie können Ihr Unternehmen aber mit relativ einfachen Maßnahmen vor diesen Risiken schützen.

1. AV-Tests
2. TOP3 2014 – Studie zu Ergebnissen von unabhängigen Tests

IHRE SICHERHEITS-CHECKLISTE

DER ERSTE SCHRITT ZUR ABSICHERUNG IHRES UNTERNEHMENS BESTEHT DARIN, IHRE EIGENE ARBEITSWEISE ZU BETRACHTEN UND HERAUSZUFINDEN, WO SICH RISIKEN REDUZIEREN LASSEN. STELLEN WIR DIE IT-SICHERHEIT IN IHREM UNTERNEHMEN ALSO EINMAL AUF DEN PRÜFSTAND:

MALWARE-SCHUTZ ✔

Genau wie bei der Unternehmensversicherung sollten Sie auch bei IT-Produkten zum Schutz Ihres Unternehmens auf hohe Qualität setzen. Wenn Sie nicht bereits leistungsfähige Software zum Schutz Ihrer Geräte vor Infektionen einsetzen, sollten Sie dies zu einer vorrangigen Aufgabe machen.

Leider reicht es nicht aus, im Internet einfach nur vorsichtig zu sein. Wir alle wissen, dass wir keine Dateianhänge von unbekannten Absendern öffnen oder Dateien von verdächtigen Websites herunterladen sollten, aber tatsächlich stammen viele Infektionen aber aus vertrauenswürdigen Quellen, die selbst manipuliert wurden.

VERHALTEN IM INTERNET ✔

Ihren Mitarbeitern die Bedeutung ihres Verhaltens im Internet klarzumachen, kann Ihnen einiges an Kopfschmerzen ersparen. Wahrscheinlich ist Ihren Mitarbeitern bewusst, dass es bestimmte Arten von Websites gibt, die sie während der Arbeit nicht aufrufen sollten. Wenn Ihre Mitarbeiter jedoch außerdem private Mobilgeräte (z. B. Smartphones oder Tablets) im Unternehmen nutzen, sind sie nach Verlassen des Büros vielleicht nicht mehr ganz so sicherheitsbewusst. Es empfiehlt sich also, nicht erwünschte oder unangemessene Websites auf beruflich genutzten Geräten zu sperren. Eine allgemeine Sensibilisierung für IT-Sicherheitsbedrohungen trägt außerdem dazu bei, die private und berufliche Nutzung der Geräte durch Ihre Mitarbeiter sicherer zu machen.

? WIE BIN ICH DAVON BETROFFEN?

Haben Sie schon einmal eine E-Mail von einem Freund oder Familienangehörigen mit einem Link erhalten, der Ihnen verdächtig vorkam, nachdem Sie darauf geklickt haben? Wenn Malware einen Computer infiziert hat, kann sie aktiv werden, ohne dass der Benutzer etwas davon mitbekommt. Darum sollten Sie selbst vertrauenswürdigen Quellen nicht blind vertrauen.

KENNWÖRTER ✔

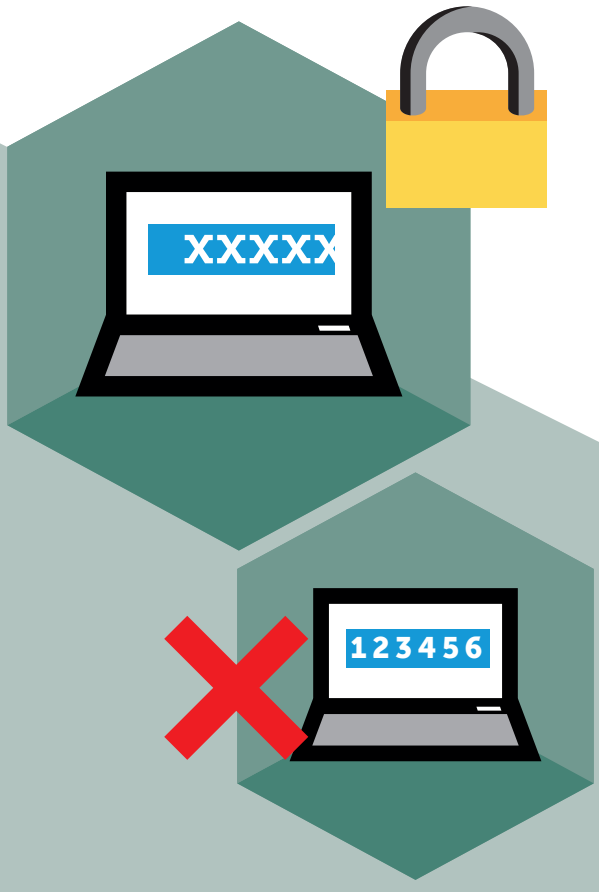
Sie sollten in Ihrem Unternehmen ausschließlich starke, eindeutige Kennwörter mit einer Mischung aus Symbolen, Zahlen und Buchstaben einsetzen. Normale Wörter lassen sich mit Programmen knacken, die einfach so lange Wörterbücher durchforsten, bis sie einen Treffer gelandet haben. Umgekehrt kann ein starkes Kennwort, das für mehrere Konten eingesetzt wird, noch größeren Schaden anrichten, sollte es geknackt werden.

UPDATES ✔

Jede Sekunde werden vier neue Malware-Objekte erkannt.[3] Nur im Nachhinein reagieren reicht da nicht. Deshalb sollten Sie automatische Updates zur täglichen Aktualisierung Ihrer Sicherheitssoftware nutzen und die übrige Software stets zeitnah aktualisieren – und sicherstellen, dass jeder im Unternehmen sich daran hält. Denken Sie daran: Programme, die nicht aktualisiert werden, sind das beliebteste Einfallstor für Kriminelle, um in ein Unternehmen einzudringen.

VERMEIDEN SIE DIESE KLASSISCHEN KENNWORT-FEHLER:

1. Verwenden von leicht zu merkenden, aber auch leicht zu ratenden Kennwörtern wie „Kennwort" oder „123456"
2. Verwenden Ihrer E-Mail-Adresse, Ihres Namens oder anderer, einfach zu beschaffender Informationen
3. Auswahl von Erinnerungsfragen, die ein Hacker mit nur wenig Recherche beantworten kann, z. B. den Mädchennamen Ihrer Mutter
4. Verwenden einfacher und offensichtlicher Abwandlungen von normalen Wörtern, z. B. indem Sie eine „1" an das Ende hängen
5. Verwenden geläufiger Phrasen. Selbst kurze Sätze wie „ichliebedich" lassen sich ziemlich schnell erraten.



Weitere Hinweise dazu, wie Sie schwer zu knackende Kennwörter erstellen, finden Sie in unserem Blogpost unter dem entsprechenden Thema.

3 AV-Tests

2014

295,500

NEUE MOBILE MALWARE-BEDROHUNGEN[4]

BANKING ✔

Von der Umleitung zu gefälschten Versionen vertrauenswürdiger Websites bis hin zum Einsatz von Malware, die Sie ausspioniert, nutzen Cyberkriminelle die unterschiedlichsten Methoden, um an Ihre Finanzdaten zu kommen. Sie müssen selbst aktiv werden, um sie aufzuhalten.

Seien Sie auf der Hut vor „Phishing"-Versuchen, bei denen sich Dritte als Ihre Bank ausgeben: Nutzen Sie stets einen sicheren Browser, und schauen Sie sich die Webadresse genau an, bevor Sie auf einer Website persönliche Informationen eingeben. Vermeiden Sie es auch, solche Informationen per E-Mail zu verschicken, da diese abgefangen werden können.

MOBILE GERÄTE ✔

Mittlerweile ist es ganz normal, von unterwegs aus zu arbeiten. Kein Wunder also, dass Mobilgeräte immer mehr zur Zielscheibe von Cyberverbrechern werden. 2014 wurden jeden Monat 295.500 neue mobile Malware-Bedrohungen entdeckt (also Schadprogramme, die speziell für Smartphones und Tablets geschrieben wurden).[5] Obwohl der Schutz von Smartphones und Tablets genauso wichtig ist, wie der von Macs und PCs, erkennen nur 32 % der Kleinunternehmen derzeit das Risiko an, das von Mobilgeräten ausgeht.[6]

VERSCHLÜSSELUNG ✔

Wenn vertrauliche Daten auf Ihren Computern gespeichert sind, sollten Sie sie verschlüsseln, damit sie bei Diebstahl oder Verlust des Geräts unbrauchbar sind. Sie sollten sich vor Augen halten, dass Ihre geschäftlichen Informationen einen sehr hohen Wert darstellen, den es zu schützen gilt.

? WAS IST PHISHING?

Beim „Phishing" geben sich Kriminelle als vertrauenswürdige Institution aus, in der Hoffnung, Sie zur Preisgabe vertraulicher Informationen, z. B. Kennwörter und Kreditkartendaten, zu bewegen, die dann für eine Betrugsmasche eingesetzt werden.

4 & 5 Laut Angabe von Kaspersky Lab
6 Umfrage zu globalen IT-Sicherheitsrisiken 2014

DIE RISIKEN VERSTEHEN

ES IST WICHTIG, ÜBER ONLINE-SICHERHEIT ZU SPRECHEN, ABER FÜR VIELE VON UNS IST DIESES THEMA EIN BUCH MIT SIEBEN SIEGELN. DIE AUSWIRKUNGEN EINES ERFOLGREICHEN ANGRIFFS, SIND OFTMALS SEHR DRASTISCH UND KÖNNEN DIE EXISTENZ EINES UNTERNEHMENS GEFÄHRDEN. WIR HABEN VERSUCHT, ES IHNEN EIN WENIG LEICHTER ZU MACHEN, UND MÖCHTEN IHNEN DIE KONSEQUENZEN – UND WIE SIE DIESE VERMEIDEN KÖNNEN – ANHAND EINIGER SZENARIEN DEMONSTRIEREN.

Ein sehr teurer Kaffee

Nachdem Thomas den letzten Kunden des Tages verabschiedet hat, überlässt er das Abschließen seinem Geschäftspartner. Direkt gegenüber dem Büro gibt es ein Café, wo er mit einem Freund verabredet ist. Als ihm einfällt, dass eine Lieferantenrechnung am nächsten Tag fällig wird, entscheidet er sich, sich darum zu kümmern, bevor er es wieder vergisst.

Über seinen Laptop verbindet er sich mit dem WiFi-Netzwerk des Cafés, meldet sich bei der Website seiner Bank an und tätigt die Überweisung. Zufrieden, dass er es nicht vergessen hat, lehnt er sich zurück und genießt seinen Kaffee.

Als er beim nächsten Mal seinen Kontostand prüft, ist das Konto leer. Während Thomas noch versucht herauszubekommen, wie dies passieren konnte, warten seine Angestellten auf ihr Gehalt.

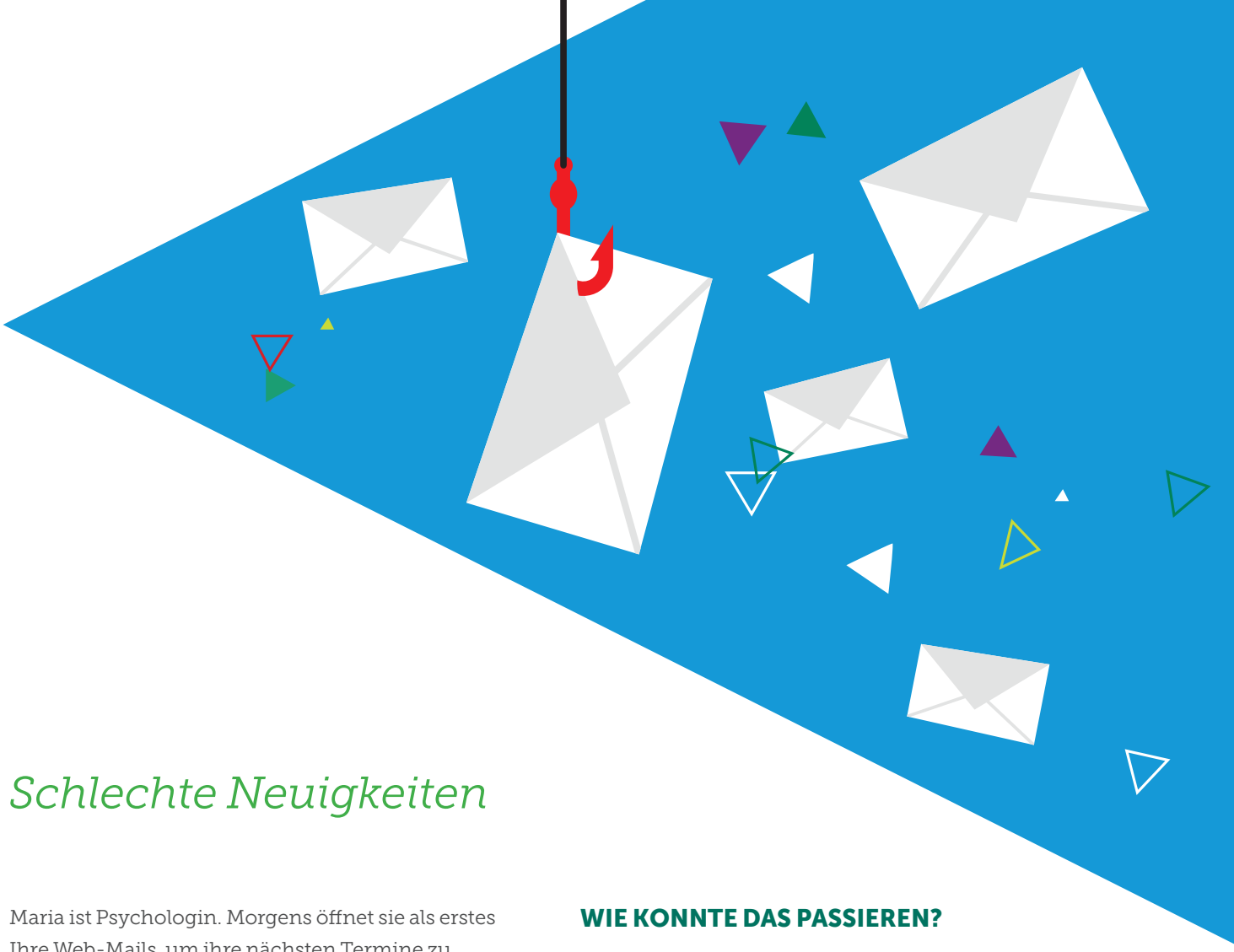
WIE KONNTE DAS PASSIEREN?

Leider hatte Thomas keinerlei Malware-Schutz installiert, und sein Laptop wurde mit einem Keylogging-Schadprogramm infiziert. Auf diese Weise wurde ein Datensatz mit allen von Thomas eingegeben Informationen an die Hacker weitergeleitet. Und da Thomas ein ungesichertes öffentliches WiFi-Netzwerk nutzte, bestand zusätzlich das Risiko, dass die Überweisung selbst abgefangen wurde.

WAS HÄTTE MAN BESSER MACHEN KÖNNEN?

Online-Banking-Geschäfte sollten nur auf Geräten mit installiertem Malware-Schutz ausgeführt werden, und das auch nur unter Verwendung eines sicheren Browsers. Mit der Technologie für den Sicheren Zahlungsverkehr von Kaspersky Lab hätte Thomas einwandfrei feststellen können, ob die Transaktion sicher war oder nicht.

Da er ein ungesichertes öffentliches Netzwerk nutzte, hätten die Daten außerdem weitaus einfacher abgefangen werden können als bei einer privaten Verbindung. Um all dies hätte er sich keine Gedanken machen müssen, wenn ihm die Funktion „Sicherer Zahlungsverkehr“ zur Verfügung gestanden hätte.



Schlechte Neuigkeiten

Maria ist Psychologin. Morgens öffnet sie als erstes Ihre Web-Mails, um ihre nächsten Termine zu überprüfen. Ganz oben im Posteingang findet sie eine Benachrichtigung von einem der Sozialen Netzwerke vor, das sie nutzt. In der E-Mail wird Maria aufgefordert, ihr vorhandenes durch ein stärkeres Kennwort zu ersetzen. Sie klickt auf den Link in der E-Mail, bestätigt das vorhandene Kennwort, und ersetzt dann jedes zweite Zeichen des alten Kennworts durch ein Sternchen.

Mit dem zufriedenen Gefühl, dass ihr Konto jetzt sicherer vor Hackern ist, befasst sie sich wieder mit ihren Mails und hat das ganze schon bald vergessen ...

... bis ihr in einem Erpresserbrief gedroht wird, die Details aller Patienten, die zu ihr in die Praxis kommen, zu veröffentlichen.

WIE KONNTE DAS PASSIEREN?

Maria ist einer Phishing-Masche zum Opfer gefallen. Obwohl die Website genauso aussah wie die, die sie schon unzählige Male zuvor besucht hatte, handelte es sich um eine Fälschung. Nachdem die Betrüger Zugriff auf Marias Profildaten hatten, stießen sie auch auf die Daten ihrer Patienten. Sie probierten dasselbe Kennwort aus, das sie aus ihr herausgelockt hatten, um an ihre beruflichen E-Mails zu gelangen. Und da Maria dasselbe Kennwort für beide Konten nutzte, konnten die Betrüger alle ihre Mails mitsamt der Anhänge lesen, von denen einer eine vollständige Patientenliste inklusive Kontaktdaten war.

WAS HÄTTE MAN BESSER MACHEN KÖNNEN?

Natürlich hätte Maria bewusst sein müssen, dass seriöse Websites und Organisationen persönliche Details nie per E-Mail anfordern. Nachdem Sie auf den Link geklickt hatte, wäre sie von einer guten Sicherheitssoftware darauf aufmerksam gemacht worden, dass die Website gefälscht war.

Ein weiterer Fehler bestand darin, dasselbe Kennwort für private und berufliche Zwecke zu nutzen.

WARUM KASPERSKY LAB?

WIR HABEN ES UNS ZUR AUFGABE GEMACHT, UNSEREN KUNDEN DEN BESTMÖGLICHEN IT-SCHUTZ ZU GEWÄHREN, DER GLEICHZEITIG EINFACH ANZUWENDEN UND ZU VERWALTEN IST. MIT KASPERSKY SMALL OFFICE SECURITY IST ES UNS GELUNGEN, UNSER KNOW-HOW IN EINER LÖSUNG ZU VEREINEN, DIE EBENSO BENUTZERFREUNDLICH WIE EFFEKTIV IST. DAMIT SIE SICH WIEDER AUF DAS KONZENTRIEREN KÖNNEN, WAS SIE AM BESTEN KÖNNEN, NÄMLICH IHR UNTERNEHMEN ZU FÜHREN.

Uns ist bewusst, dass Kleinunternehmen beim Thema Cybersicherheit eine Sonderstellung einnehmen. Sie müssen oft denselben Bedrohungen entgegentreten wie Großunternehmen, sind aber in vielerlei Hinsicht ähnlich anfällig wie Privatanwender. Wir glauben, dass diese Sonderstellung einen speziellen Sicherheitsansatz verlangt.

Ein Endverbraucherprodukt für die Nutzung durch Kleinunternehmen einfach in eine neue Verpackung zu stecken, ist nicht angemessen. Eine solche Lösung bietet beispielsweise keinen Schutz für Server, wird aber in vielen Kleinunternehmen aktuell oder in absehbarer Zukunft eingesetzt. Im Gegensatz zu Privatanwendern benötigen Unternehmen unkomplizierten Schutz für mehrere Geräte.

Eine Lösung, die für Großunternehmen vorgesehen ist, einfach nur „abzuspecken" funktioniert jedoch auch nicht. Kleinunternehmen haben keine speziellen IT-Mitarbeiter oder die Zeit, sich mit komplizierter Spezial-Software auseinanderzusetzen.

Kaspersky Small Office Security besitzt alle erforderlichen Funktionen, ist aber trotzdem einfach und unkompliziert. Die Lösung bremst Sie nicht aus und deckt eine große Bandbreite unterschiedlicher Geräte ab. So genießen Sie effektiven Schutz, wo immer Sie auch geschäftlich unterwegs sind.

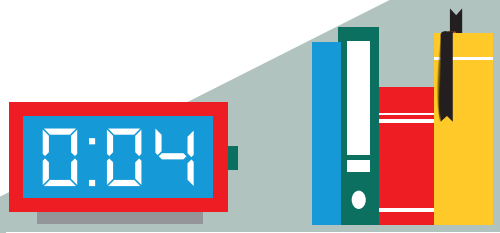
KANN ICH MICH NICHT KOSTENLOS SCHÜTZEN?

Es gibt zwar eine Reihe von kostenlosen Sicherheitslösungen, aber diese bieten einfach keinen umfassenden Schutz. Manche der kostenlosen Anwendungen lassen bewusst Spielraum für Verbesserungen. Auf diese Weise soll der Benutzer dazu gebracht werden, ein Upgrade auf die Bezahlversion auszuführen.

Wenn die Sicherheit Ihres Unternehmens auf dem Spiel steht, sollte nur optimaler Schutz für Sie in Frage kommen, und zwar von Anfang an.

PROAKTIVE MASSNAHMEN

NACHDEM WIR NUN DIE BEREICHE ABGESTECKT HABEN, DIE SIE FÜR IHRE SICHERHEITSSTRATEGIE BERÜCKSICHTIGEN SOLLTEN, WIRD ES ZEIT, SICH ZU ÜBERLEGEN, WIE SIE DIESE MITHILFE EINER MASSGESCHNEIDERTEN LÖSUNG UMSETZEN.



REGELMÄSSIGE AKTUALISIERUNGEN SICHERSTELLEN

Bei Kaspersky Small Office Security brauchen Sie sich keine Sorgen zu machen. Wir aktualisieren Ihren Schutz in Echtzeit. Damit sind Sie auch vor aufkommenden Bedrohungen immer optimal geschützt.

NUTZUNG STARKER KENNWÖRTER ERZWINGEN

Machen Sie Ihren Mitarbeitern das Leben einfach – mit dem Kaspersky Passwort Manager. Diese Komponente generiert automatisch starke Kennwörter und speichert sie in einer verschlüsselten Datenbank. Sie brauchen sich also nur noch ein einziges Kennwort zu merken, erhöhen Ihre Sicherheit aber erheblich.

VERSCHLÜSSELUNG UND SICHERUNG VERTRAULICHER/ KRITISCHER DATEN

Mit Kaspersky Small Office Security können Sie Ihre vertraulichen und wichtigen Informationen in speziellen verschlüsselten Speichern ablegen. Dank der Wiederherstellungsfunktion gehen Ihre wichtigen Daten selbst dann nicht verloren, wenn Computer oder Server abstürzen.

SCHUTZ FÜR ALLE IHRE GERÄTE

Kaspersky Small Office Security bietet Schutz für unterstützte Tablets und Smartphones. Und wenn ein Gerät einmal abhanden kommt oder gestohlen wird, hilft die Lösung Ihnen dabei, es wiederzufinden und vertrauliche Informationen per Fernzugriff zu löschen.

SCHUTZ VOR KRIMINELLEN

Unsere vielfach ausgezeichnete Funktion „Sicherer Zahlungsverkehr" wird mit nur wenigen Klicks aktiviert und ermöglicht hochsicheres Browsen. Sie ermittelt, ob die von Ihnen genutzten Websites manipuliert wurden. Auf diese Weise können Sie das Risiko einer Sicherheitsverletzung von vornherein ausschließen. Gleichzeitig sorgen unser Malware- und Phishing-Schutz und unsere Firewall dafür, dass Sie während Ihrer übrigen Online-Aktivitäten von Kriminellen unbehelligt bleiben.

SCHÜTZEN SIE JETZT IHR UNTERNEHMEN.

Kaspersky Small Office Security ist für die individuellen Anforderungen kleiner Unternehmen ausgelegt und verbindet effektiven Schutz mit Benutzerfreundlichkeit, was besonders für Unternehmen wie Ihres von großem Vorteil ist.

Besuchen Sie **www.kaspersky.com/de/IT-Sicherheit-fuer-kleine-Unternehmen**, und finden Sie heraus, wie Sie Ihr Unternehmen mit Kaspersky Small Office Security schützen können.

SCHÜTZEN SIE JETZT IHR UNTERNEHMEN

DEM GESPRÄCH BEITRETEN

#protectmybiz

Auf YouTube ansehen

Werden Sie unser Fan auf Facebook

Lesen Sie unseren Blog

Folgen Sie uns auf Twitter

Treten Sie uns auf LinkedIn bei

Weitere Informationen erhalten Sie unter www.kaspersky.com/de/IT-Sicherheit-fuer-kleine-Unternehmen

ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer*. In seiner 17-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Der Hauptsitz des Unternehmens ist in Großbritannien registriert. Kaspersky Lab ist zurzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 400 Millionen Anwendern weltweit. Weitere Informationen erhalten Sie unter: www.kaspersky.de.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2013" den vierten Rang. Die Rangfolge wurde im IDC-Bericht „Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares" (IDC Nr. 250210, August 2014) veröffentlicht. In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2013 eingestuft.