Reputation und Cybersicherheit: Vom Risiko zur Chance

kaspersky

Reputation und Cybersicherheit: Vom Risiko zur Chance

„Es kann Jahre dauern, sich einen guten Ruf aufzubauen – und nur fünf Minuten, ihn zu ruinieren. Wer das verinnerlicht, geht die Dinge anders an.“ (Warren Buffett)

Die Grenzen der Angst als Motivator – Einblicke aus der Psychologie

Angst ist nützlich. Laut Neurowissenschaftlern im Karolinska-Krankenhaus in Stockholm, ist es die „Funktion von Angst, Organismen dazu zu motivieren, mit Bedrohungen umzugehen, die während der Evolution eine Gefahr fürs Überleben darstellten“.

Doch die durch Angst ausgelösten Schutzmechanismen, also Erstarren, Kämpfen oder Flüchten, sind für den modernen Arbeitsplatz nicht geeignet. Wir bekämpfen zwar Cyberbedrohungen, aber abseits dieses Kontexts ist die durch Angst ausgelöste Kampfreaktion ein sehr einfaches Instrument, das immer kurzfristig gedacht ist.

Psychologin

Christine Tappolet (Université de Montréal) drückt es wie folgt aus: „Angst beeinflusst, was wir tun, indem sie den Fokus des Handelnden [also unseren] einschränkt.“ Wir konzentrieren uns nur auf das, was unmittelbar vor uns liegt, und können so das große Ganze nicht sehen.

In der Psychologie wird zwischen der Annäherungsmotivation (Anziehung durch etwas Positives, angetrieben durch Hoffnung) und der Vermeidungsmotivation (Wegbewegen von etwas Negativem, angetrieben durch Angst) unterschieden. Beide spielen eine wichtige Rolle, doch laut Andrew Elliot (University of Rochester) soll die „Vermeidungsmotivation das Überleben sicherstellen, während die Annäherungsmotivation dafür sorgt, dass dieses Leben auch gedeiht“.

Mit diesem Bericht möchten wir Sie dabei unterstützen, das reine Überleben hinter sich zu lassen und die Chance zu nutzen, eine starke und überzeugende Reputation aufzubauen, die durch Ihren zuverlässigen Sicherheitsansatz und Ihren Cyberstolz gestützt wird.

Beginnen wir mit einer grundlegenden Tatsache: Cybervorfälle können dem Ruf eines Unternehmens schaden. Der Grund ist einfach: Kunden erwarten, dass Sie ihre Daten schützen und dass Services stets verfügbar sind. Wenn das nicht funktioniert, suchen sie sich schnell einen anderen Anbieter. Und das Risiko einer Rufschädigung durch Cybervorfälle steigt stetig.

Die Relevanz der Reputation eines Unternehmens ist nichts Neues: Der Ruf war schon immer eines der wichtigsten Assets für ein Unternehmen. Kunden kaufen nicht einfach eine Lösung, einen Service oder ein Produkt; sie kaufen eine Marke, eine Idee oder ein Versprechen von etwas Größerem. Vertrauen ist dabei oft der entscheidende Faktor.

Im digitalen Zeitalter ist der Schutz des guten Rufes wichtiger als je zuvor und das aus zwei Gründen: Der erste ist Cyberkriminalität: Angreifer versuchen, Unternehmen aus der Ferne in die Knie zu zwingen. Der zweite Grund setzt sich aus dem digitalen Kontext von Social Media, der sofortigen Verfügbarkeit von Informationen sowie offenen Bewertungsseiten wie z. B. Trustpilot, G2 oder Feefo zusammen. Das alles sorgt dafür, dass die Front für die Abwehr von Bedrohungen nicht nur immer breiter wird, sondern auch immer undeutlicher definiert ist. Und es verstärkt zusätzlich die Herausforderung, negative Nachrichten im Zaum zu halten (selbst wenn es nur Gerüchte sind).

Entdecken Sie mit uns nicht nur die Risiken, sondern auch die Chancen von Reputationsmanagement und Cybersicherheit

Imageschäden aus Cybervorfällen sind ein wichtiges Thema. In diesem Bericht stellen wir Ihnen einige Fakten vor, die Sie kennen müssen, um den guten Ruf Ihres Unternehmens heute und in Zukunft zu schützen.

Wir betrachten außerdem das Zusammenspiel zwischen Cybersicherheit und Reputation aus einem völlig neuen Blickwinkel – einem, der bisher in der Diskussion dieses Themas fehlt. Neben wichtigen Informationen zu möglichen Risiken stellen wir Ihnen auch die Möglichkeiten vor, die das Thema Unternehmensimage im Kontext der Cybersicherheit und darüber hinaus bereithält.

Wir glauben, dass eine rein defensive Position nicht ausreicht: Sie wird Ihrem Unternehmen, Ihren Kunden, Ihren Zielen und Ihren Werten nicht gerecht. Stattdessen möchten wir Ihnen ein völlig neues Konzept vorstellen: Wir nennen es „Cyber-Selbstbewusstsein“. Mit diesem Ansatz möchten wir erreichen, dass wir nicht mehr nur aus Angst vor Bedrohungen handeln, sondern uns über diese rein defensive Position hinaus entwickeln – hin zu einer Welt, in der Reputation wertgeschätzt, kultiviert und zelebriert wird, anstatt sie nur zu bewachen.

Vorstellung der drei Reputationsbereiche

Der Unternehmensruf ist ein komplexes Konstrukt. Er wird durch die kumulativen Aktionen in drei Bereichen aufgebaut und kann durch Problemen in diesen Bereichen auch wieder zerstört werden. Die Bereiche lauten wie folgt (Reihenfolge nicht relevant):

1. Produkt
2. Branding
3. Sicherheit

In diesem Bericht liegt unser Fokus hauptsächlich auf dem dritten Bereich: der Sicherheit. Wir behandeln jedoch auch die beiden ersten Bereiche kurz, um das Zusammenspiel der drei zu verdeutlichen.

Reputationsbereich 1: Produkt

Dieser Bereich ist einfach erklärt: Wenn Ihr Produkt gut ist, wissen Ihre Kunden das und ziehen Sie Ihrer Konkurrenz vor. In einer idealen Welt würde der Ruf ausschließlich vom Produkt abhängen. Wäre es nicht toll, wenn wir einfach nur ein gutes Produkt entwickeln müssten, das sich dann quasi von allein verkauft?

Vertrauen ist alles
Wenn Ihre Kunden etwas von Ihnen kaufen, übertragen sie im Gegenzug für Produkte oder Services Geld auf Ihr Konto. Das passiert jedoch nur, wenn Kunden dem jeweiligen Anbieter seine Versprechen auch abnehmen. Dementsprechend hat das Vertrauen der Kunden starken Einfluss auf Kaufentscheidungen – von Verbrauchern bis hin zu den größten Unternehmen. Ihre Kunden entscheiden sich für Ihre Produkte, weil sie darauf vertrauen, dass Sie besser sind als die Konkurrenz. Dieses Vertrauen wird durch eine der wertvollsten Ressourcen gestärkt, die ein Unternehmen haben kann: seinen Ruf.

Weitere Folgen schlechter Reputation
Wir dürfen nicht vergessen, dass Ihre Kunden nicht die einzige Gruppe sind, für die Ihr Ruf entscheidend ist. Unternehmen benötigen auch Zugang zu Krediten – eine schlechte Reputation beeinträchtigt jedoch die Kreditwürdigkeit und erschwert so Investitionen und Wachstum. Und auch Versicherungsbeiträge können durch Rufschäden steigen, da Versicherer bei Unternehmen, deren Reputation in Sachen Cybersicherheit zu wünschen übrig lässt, mehr berechnen.

Reputationsbereich 2: Branding

Branding ist ein jüngerer Bereich, dessen Einfluss auf den Ruf Ihres Unternehmens weiter zunimmt, je stärker der potentielle Markt wächst und je kleiner die Welt durch das Internet wird. Beim Branding geht es darum, dass Kunden mehr als nur ein Produkt kaufen: Sie kaufen eine Idee oder manchmal sogar nur ein Gefühl der Zugehörigkeit. Wenn Ihr Produkt gut ist, aber das Branding nicht, können Sie entwickeln, so viel Sie wollen – die Kunden werden ausbleiben.

Reputationsbereich 3: Sicherheit

In der Regel hören Sie zu diesem Bereich, dass er in der Lage ist, den guten Ruf aus Produkten und Branding vollkommen zu zerstören, wenn die richtige Sicherheit fehlt und es so zu einem erfolgreichen Cyberangriff kommt. In diesem Bericht werfen wir einen anderen Blick auf das Thema Sicherheit. Allerdings stimmt es natürlich, dass die Imageschäden, die mit diesem Bereich einhergehen, tatsächlich den guten Ruf aus Produkten und Branding zunichte machen können.

Ab jetzt konzentrieren wir uns aber auf das Positive. Der Bereich der Sicherheit umfasst drei wichtige Bereiche, die wir unten zusammengefasst haben – gemeinsam mit Fragen, die Ihren Kunden dazu durch den Kopf gehen:

- Kundendaten: „Respektiert mich das Unternehmen?“
- Zuverlässige Verfügbarkeit (statt Latenz): „Kann ich mich darauf verlassen, dass das Unternehmen immer den versprochenen Service bietet?“
- Kompetenz: „Weiß das Unternehmen überhaupt, was es tut?“

Zum Einstieg einige Fakten

Der Unternehmensruf kommt bei IT-Sicherheits- oder anderen Geschäftsstrategien oft zu kurz. Dabei ist unsere Reputation wie das Gold in unserem Fort Knox. Durch ihn vertrauen Kunden darauf, dass unsere Produkte und Services nicht nur ihre Erwartungen erfüllen, sondern auch die Angebote unserer Konkurrenz übertreffen. Und das Wichtigste für diesen Ruf ist das **Vertrauen.**

Warum wir wissen, was wir wissen: Internationale Kaspersky-Umfrage zu IT-Sicherheitsrisiken

Seit neun Jahren führt Kaspersky regelmäßig internationale Umfragen zur IT-Sicherheitsrisiken in Unternehmen durch, um herauszufinden, was genau sie bei Sicherheitsvorfällen durchmachen. Die Umfragen decken 23 Länder ab und umfassen Daten aus über 5000 Befragungen mit Führungskräften aus Unternehmen aller Bereiche. Auf die Daten aus dieser umfangreichen Studie stützen wir unsere Entscheidungen, um zu gewährleisten, dass unsere Produkte und Services auch weiterhin die realen Probleme unserer Kunden lösen.

Die Verbindung zwischen Sicherheit und Geschäftserfolg – Fakten aus unserer Studie

Wenn es um den Unternehmensruf geht, lässt man sich von dem Mehrwert, den er bietet, schnell dazu hinreißen, sich in oberflächlichem Marketingfloskeln zu verlieren. Nicht dass Marketing keine wichtige Rolle spielen würde, aber es ist letztlich das Ergebnis, das zählt. Deshalb untersucht unsere Studie die exakten finanziellen Folgen von Sicherheitsvorfällen. Schließlich müssen wir die Gefahr kennen, wenn wir sie bewältigen wollen.

In diesem Bericht sehen wir uns vier Kategorien an, die für die finanziellen Verluste verantwortlich sind, die bei Imageschäden durch Cybervorfälle entstehen:

1. Entgangene Aufträge
2. Schäden bei der Bonitätsbewertung und Anstieg von Versicherungsbeiträgen
3. PR-Kosten für Schadensbegrenzung und Wiederherstellung des guten Rufes
4. Entschädigungskosten (eine Entschuldigung finanzieller Natur)

Durchschnittliche Cybervorfälle in KMUs und Großunternehmen schlüsseln sich wie folgt in diese vier Bereiche auf:

Verlustkategorie	KMUs 2019	Großunternehmen 2019
Entgangene Aufträge	13 000 USD	163 000 USD
Kreditwürdigkeit/Versicherungsbeiträge	13 000 USD	179 000 USD
PR-Kosten	12 000 USD	161 000 USD
Entschädigungen	5000 USD	72 000 USD
Reputationsverluste GESAMT	43 000 USD	575 000 USD
Verlust GESAMT pro Cybervorfall	108 000 USD	1,4 Mio. USD
% des Verlusts durch Reputation	40 %	41 %

Die Folgen finanzieller Verluste durch PR-Probleme
Nachdem wir bereits die finanziellen Verluste vorgestellt haben, die durch Cybervorfälle entstehen, untersuchen wir im Folgenden auch die Folgen, die diese Verluste für Unternehmen haben. Wir haben die Umfrageteilnehmer gefragt, ob ihr Unternehmen in den letzten zwölf Monaten PR-bezogene Probleme (Skandale, öffentliche Krisen) erlebt hat – aufgrund von allgemeinen Sicherheitsvorfällen oder insbesondere durch Datenschutzverletzungen. Außerdem haben wir sie darum gebeten, die entsprechenden Verluste für ihr Unternehmen zu beziffern.

Von den Unternehmen, die allgemeine Sicherheitsvorfälle erlebt haben, gaben 77 Prozent an, dass diese Vorfälle große oder sogar sehr große finanzielle Verluste durch PR-Probleme verursacht haben. Bei den Unternehmen mit Datenschutzverletzungen waren es sogar 80 Prozent. Der Anteil war bei KMUs derselbe wie bei Großunternehmen.

Es ist wenig überraschend, dass Versicherungsunternehmen mittlerweile vermehrt PR-Support im Rahmen ihrer Servicepakete anbieten, um Unternehmen nach Cybervorfällen zu unterstützen. Hiscox (UK) berichtete hierzu:

PR-Kosten:
Die nach unserer vorherigen schriftlichen Vereinbarung entstanden Kosten für folgende Bereiche:

1. **Berater für PR oder Krisenmanagement, der Sie bei der Wiederherstellung Ihres Unternehmensrufes und der Reaktion auf Medienberichte unterstützt, einschließlich der Entwicklung und Kommunikation einer Wiederherstellungsstrategie**
2. **Versenden oder Veröffentlichen von Statements per E-Mail, auf Ihrer Webseite oder in Social Media, einschließlich der Verwaltung und Überwachung Ihrer Social Media-Konten**
3. **Andere angemessene Maßnahmen zum Schutz oder zur Wiederherstellung Ihres Unternehmensrufes**

Am überraschendsten ist hierbei die Tatsache, dass 40 Prozent aller finanziellen Verluste, die Unternehmen bei Cybervorfällen entstehen, nur auf die damit verbundenen Imageschäden zurückzuführen sind. Die verbleibenden 60 Prozent gehen durch Beauftragung externer Experten, zusätzliche Gehälter, Strafen und Gebühren, Software- und Infrastrukturverbesserungen, Schulungen sowie die Einstellung neuer Mitarbeiter verloren.

Wenn wir also die Reputation isoliert betrachten, können Unternehmen durch den Schutz ihres Rufes theoretisch 40 Prozent der finanziellen Folgen von Cybervorfällen einsparen. Natürlich ist das in der Realität nicht umsetzbar, da der gute Ruf solider Cybersicherheit auf Fakten basiert und nicht auf gutem Marketing. Diese Zahl zeigt jedoch, wie wichtig es ist, Imageschäden zu verhindern.

Ein ganzheitlicher Ansatz für das reale Heute und Morgen

Wir wissen, dass die drei Bereiche der Reputation eng miteinander verbunden sind und deshalb nicht getrennt voneinander behandelt werden können. Das sind gute Nachrichten: Denn hierdurch wirken sich Investitionen zur Verbesserung von Ruf und Gewinn im einen Bereich auch positiv auf die anderen beiden Bereiche aus. Hierfür müssen wir uns jedoch von der negativen Sichtweise auf Cybersicherheit als reine Verteidigungstaktik verabschieden. Und auch von Lösungen, für die nur die interne IT verantwortlich ist.

Cybersicherheit ist zwar ein verhältnismäßig neues Problem, doch das übergeordnete Thema – **wie Unternehmen zu ihrem Vorteil Risiken minimieren** – ist ein Thema, seit es Unternehmen gibt. Um unseren Ansatz für Cybersicherheit zu perfektionieren, müssen wir das Rad nicht neu erfinden. Wenn wir eine weitere Branche betrachten, die sich erfolgreich ihren Risiken gestellt hat und sogar daran gewachsen ist, wird deutlich, warum wir mit diesem Ansatz richtig liegen.

Was wir von der Automobilbranche über Cybersicherheit und Reputation lernen können

1869 kam Mary Ward, eine irische Wissenschaftlerin, als erster Mensch bei einem Autounfall ums Leben. Nur 150 Jahre später belegen diese Unfälle Platz 9 auf der Liste der häufigsten Todesursachen: 1,2 Millionen Menschen sterben jedes Jahr im Straßenverkehr. Das Risiko wird erst wirklich deutlich, wenn man bedenkt, dass wir derzeit geschätzte 1,4 Milliarden Fahrzeuge auf der Welt haben und jedes Jahr 74 Millionen verkauft werden.

Das zeigt, dass die Risiken, mit denen Automobilhersteller und ihre Kunden zu kämpfen haben, deutlich höher sind als bei Cybervorfällen: Denn hier geht es um schwere Verletzungs- oder sogar Lebensgefahr. Dagegen wirkt eine Datenschutzverletzung nicht mehr sonderlich bedrohlich. Aus dieser Sicht heraus ist es eher überraschend, dass Automobilhersteller in ihren aktuellen Werbe- und PR-Kampagnen Sicherheit als eines der wichtigsten Themen einsetzen. Stellen Sie sich Ihr eigenes Unternehmen und die Risiken vor, die Cybervorfälle für Sie bedeuten? Würden Sie eine Image-Kampagne mit dem Bereich Sicherheit starten? Zu viele Unternehmen hoffen lieber, dass ihre Kunden das Thema Cybersicherheit beim Kauf ignorieren und anschließend kein Cybervorfall auftritt. Und wenn doch, beschäftigen sie sich eben dann damit.

Natürlich war auch die Autobranche nicht immer so mutig. Während die Risiken – oder nennen wir es beim Namen: die Todeszahlen – über Jahrzehnte immer weiter exponentiell anstiegen, versuchten die Hersteller, Kunden mit anderen Werten und Merkmalen abzulenken: Glamour, Freiheit, Spaß, Luxus und natürlich Motorleistung. Fahrzeughersteller haben das Thema Sicherheit erst in den 80er Jahren in ihr Marketingrepertoire aufgenommen. Damals fingen sie an, ihre proaktiven Schutzmaßnahmen als integralen Bestandteil nicht nur ihrer Produkte, sondern der gesamten Marke zu bewerben.

Viele moderne Unternehmen sind in Sachen Cybersicherheit und Reputationsmanagement von Bedenken getrieben und sehen daher – ähnlich wie die Fahrzeugbranche damals – im Thema Sicherheit eines der größten Risiken für erfolgreiche Verkäufe. Durch diese Angst, die durch Unsicherheit hinsichtlich der rasanten Entwicklung im Bereich der Cyberrisiken noch weiter verstärkt wird, können Unternehmen jedoch schnell riesige Wachstumschancen verpassen.

Nehmen wir zum Beispiel Volvo. Das Unternehmen ist laut öffentlicher Meinung und einigen unabhängigen Tests seit Jahrzehnten einer der sichersten Fahrzeughersteller. Und das ist kein Zufall: Volvo war eines der ersten Unternehmen, die das positive und rentable Verhältnis zwischen Sicherheit und Reputation verstanden hat, und veröffentlichte dementsprechend eine völlig individuelle und mutige Kampagne mit Crashtest-Dummys. Die 1987er Werbung für den Volvo 340 lohnt sich auch heute noch: elegante 43 Sekunden, die optimal veranschaulichen, warum Unternehmen Sicherheit ins Rampenlicht rücken müssen – auch die Cybersicherheit.

Letztes Jahr setzte auch Toyota in seiner „New Gig"-Werbekampagne auf die Unterstützung eines Crashtest-Dummys, um die Sicherheit zu bewerben. Dieser Dummy ist jedoch traurig darüber, dass er dank der vielen automatisierten Sicherheitsfunktionen von Toyota, die Unfälle gar nicht erst passieren lassen, nun seinen Job los ist.

Volvos Sicherheitsruf basiert auf grundsoliden Sicherheitstechnologien und fördert so das Wachstum

Volvos Ruf für Sicherheit ist nicht einfach nur durch eine Werbekampagne entstanden. Die Kampagne konnte nur funktionieren, weil die darin enthaltenen Aussagen wahr sind und auch unabhängige Tests das immer wieder bestätigen. So wurde der Volvo XC90 im Jahr 2017 tatsächlich als sicherstes Auto der Welt ausgezeichnet – und das von einer der hochrangigsten unabhängigen Prüfstellen überhaupt: dem US-amerikanischen Insurance Institute for Highway Safety (IIHS).

Wenn es darum geht, nicht nur überzeugende Werbung, sondern auch Leistung zu bringen, unterscheidet sich Cybersicherheit nicht von der Fahrzeugsicherheit. Und das ist in zweierlei Hinsicht relevant: Zunächst einmal können Sie in dem Wissen, dass Ihr Unternehmen sicher ist, das Thema Sicherheit selbstsicher als wichtiges Merkmal vermarkten und Ihre Aussagen durch Fakten stützen. Der offensichtlichere Faktor ist jedoch, dass Kunden früher oder später herausfinden, ob Anbieter nur viel versprechen oder ihre Versprechen auch einhalten. Das kann zum einen durch Cybervorfälle passieren, die den entsprechenden Service beeinträchtigen oder bei denen Daten gestohlen werden. Es liegt zum anderen aber auch daran, dass Verbraucher immer besser darin werden, falsche Versprechungen zu erkennen. Immer häufiger decken sie falsche Behauptungen auf oder verlangen Belege für Marketing-Behauptungen.

Bevor wir nun besprechen, wie Kaspersky Sie dabei unterstützen kann, das Thema Sicherheit selbstsicher als wichtiges Merkmal zu vermarkten und so das Wachstum zu fördern und das Vertrauen Ihrer Kunden zu steigern, möchten wir Ihnen gern zeigen, dass auch wir nicht nur leere Versprechungen machen. Denn Behauptungen aufzustellen, ist einfach. Wenn sie jedoch nicht auf Fakten basieren, wie es beim Volvo XC90 und dem IIHS der Fall war, sind diese Behauptungen wertlos.

Deshalb sind wir stolz auf unsere häufig getesteten und vielfach ausgezeichneten Cybersicherheitslösungen, mit denen wir regelmäßig Top-Ergebnisse in zahlreichen unabhängigen Tests erzielen. Diese konstante Leistung sagt mehr aus als einzelne Erfolge.

Unter diesen Auszeichnungen finden sich einige Anerkennungen, auf die wir besonders stolz sind und die wir Ihnen deshalb gern vorstellen möchten:

- Die Globale Transparenzrichtlinie von Kaspersky wurde kürzlich vom Paris Call for Trust and Security in Cyberspace empfohlen (siehe links).
- AV-Comparatives gratulierte Kaspersky vor Kurzem für den Award als „Top Rated Product" sowie andere Auszeichnungen im Jahr 2019.
- Im Advanced Threat Defense Test von ICSA Labs für das dritte Quartal 2019 war Kaspersky Anti Targeted Attack Platform die einzige Lösung, die eine Erkennungsrate von 100 Prozent und null False Positives erzielte.
- In diesem Jahr erhielt Kaspersky die Zertifizierung nach ISO/IEC 27001:2013, eine internationale Norm, die Best Practices für Systeme zur Verwaltung der Informationssicherheit festlegt.

Das sind nur einige der Auszeichnungen, dank denen wir unseren 400 Millionen Nutzern und 270 000 Unternehmenskunden selbstbewusst sagen können: **„Ihr könnt euch auf uns verlassen; ihr seid geschützt."**

Und wir möchten gern erreichen, dass auch Sie und Ihr Unternehmen diese Selbstsicherheit aufbauen, damit Sie sich von der Masse abheben und selbstbewusst sagen können, wie wichtig Ihnen die Sicherheit von Kundendaten ist – in der Sicherheit, dass Sie Ihre Versprechen auch einhalten können. Doch durch den anhaltenden Mangel an Cybersicherheitsressourcen sowie durch knappe Budgets fällt es oft schwer, diese Selbstsicherheit, die wir als „Cyber-Selbstbewusstsein" bezeichnen, auf eine Weise aufzubauen, die bei Kunden Anklang findet.

Deshalb haben wir Kaspersky Endpoint Security Cloud entwickelt, um Ihnen zukunftssicheren Schutz zu bieten, der sich ganz einfach verwalten lässt. Die Lösung bietet zahlreiche Next Generation-Technologien, von denen wir Ihnen gleich mehr berichten. Zunächst wollen wir uns jedoch näher mit einer der unserer Meinung nach größten verpassten Chancen der Wirtschaftsgeschichte befassen.

Der Paris Call for Trust and Security in Cyberspace wurde 2018 von Präsident Emmanuel Macron während des Internet Governance Forum der UNESCO und des Paris Peace Forum vorgestellt. Das Programm lädt alle, die im Cyberspace tätig sind, zur Zusammenarbeit ein und hält Staaten dazu an, mit Partnern aus dem privaten Sektor, aus der Forschung und aus der Gesellschaft zu kooperieren. Und in diesem Programm wird die Globale Transparenzinitiative von Kaspersky als beispielhafte Lösung für Prinzip 6 (Lebenszyklussicherheit) genannt.

„Kaspersky implementiert einen einzigartigen Ansatz für mehr Transparenz und nachweisbares Vertrauen in die Cybersicherheit:
Die Globale Transparenzinitiative (GTI) umfasst klare Maßnahmen zur Verifikation und Risikominimierung, um das Vertrauen der Nutzer zu steigern und zu gewährleisten, dass die Cybersicherheitslösungen die Normen hinsichtlich Datensicherheit und -schutz erfüllen und übertreffen."

Warum führen Unternehmen Kampagnen nicht mit Cybersicherheit und Datenschutz an? Wo bleibt das Cyber-Selbstbewusstsein?

Laut Forrester vertraut ein Drittel der erwachsenen Internetnutzer – 32 Prozent in Großbritannien, 35 Prozent in den USA und in Deutschland und 38 Prozent in Frankreich – keinem Unternehmen beim Schutz ihrer persönlichen Daten. Darüber hinaus wissen wir, dass dieses (fehlende) Vertrauen ein wichtiger Faktor bei Kaufentscheidungen ist. Angesichts dieser Tatsache ist es überraschend, dass viele Unternehmen die Chance verpassen, die Bedenken hinsichtlich Datenschutz und Cybersicherheit in der Kommunikation mit ihren Kunden anzusprechen.

Raus aus dem Kleingedruckten

Bei vielen Unternehmen verstecken sich im Kleingedruckten der Datenschutzhinweise, die oft nur über einen Link unten auf der Webseite zu erreichen sind, wertvolle Marketinginformationen. Stattdessen sollten Unternehmen diese Informationen besser sammeln, aufarbeiten und dann gut sichtbar präsentieren.

Der durchschnittliche Datenschutzhinweis enthält eine kurze Einleitung, die berechtigte Bedenken von Kunden zum Umgang mit ihren persönlichen Informationen anspricht. Dieser Einleitung folgen jedoch meist Unmengen an rechtlichen Informationen, die für Kunden wenig ansprechend sind und nur vereinzelt explizite Aussagen darüber enthalten, wie wichtig dem Unternehmen Kundendaten und ihre Sicherheit sind.

Datenschutz und Cybersicherheit müssen zwar nicht auf jeder einzelnen Webseite und in sämtlichen Marketingmaterialien das Hauptthema sein, sie sollten jedoch auch nicht tief im Kleingedruckten des Datenschutzhinweises versteckt werden. Diese beiden Bereiche müssen im gesamten Unternehmen auf ganzheitliche Weise integriert werden und sollten als Chance für Geschäftswachstum angesehen werden – und nicht als lästige Auflage.

Vorschriften dürfen nie die einzige Grundlage für Cybersicherheit und Datenschutz sein

Viele Unternehmen glauben, dass die geltenden Bestimmungen als Grundlage für Entscheidungen zu Cybersicherheit und Datenschutz ausreichen. Das führt jedoch dazu, dass diese Entscheidungen nur auf Angst und dem Wunsch basieren, Schäden zu vermeiden.

Zunächst einmal können aktuelle Bestimmungen nur schwer mit der rasanten technologischen Entwicklung mithalten – weder auf Unternehmensseite noch auf Seite der Cyberkriminellen, die immer neue Methoden finden, um Chaos zu stiften. Vorschriften müssen selbstverständlich eingehalten werden, die Unternehmensleitung sollte aber über aktuelle Bestimmungen hinausblicken und sich stattdessen an technologische Innovationen und die ethischen Prinzipien halten, die den Vorschriften zugrunde liegen.

Die gute Nachricht ist: Wenn Unternehmen Ethik ins Zentrum von Cybersicherheit und Datenschutz rücken, wie es die Analysten von Forrester getan haben, schaffen sie hierdurch eine riesige Chance, die ethischen Werte ihrer Marke basierend auf Fakten zu vermarkten. Das ist ein konkretes Beispiel für das Zusammenspiel zwischen den Reputationsbereichen Sicherheit und Branding.

Es ist eine Sache, Kunden zu versprechen, ihre Daten mit dem größtmöglichen Respekt zu behandeln und ihnen zu zeigen, wie die verschiedenen relevanten Bestimmungen eingehalten werden. Aber es ist etwas ganz anderes, einen von Grund auf ethischen und ganzheitlichen Ansatz für Cybersicherheit und Datenschutz als wichtiges Merkmal in Ihr Produkt oder Ihre Marke zu integrieren. Wenn Entscheidungen zu Cybersicherheit und Datenschutz auf tief verankerten ethischen Werten und nicht auf Bestimmungen basieren, geht die Marketingbotschaft zum Respekt für Kundendaten über die bloße Einhaltung der Vorschriften hinaus und wirkt auf Kunden und Interessenten deutlich überzeugender.

Kurz gesagt: Wenn Sie Cybersicherheit und Datenschutz für das Geschäftswachstum nutzen möchten, dann sagen Sie nicht einfach, dass Daten Ihnen wichtig sind, sondern zeigen Sie es auch. Sie müssen das Thema Sicherheit tief verinnerlichen – in Ihren Produkten und im Unternehmen als Ganzes – und jeder spielt dabei eine Rolle. Unternehmen, die dieses einfache Ziel erreichen (wie es bei Volvo mit der Fahrzeugsicherheit der Fall ist), schaffen einen großen und vor allem langfristigen Wettbewerbsvorteil gegenüber ihrer Konkurrenz, die sich weiterhin zu stark auf Bestimmungen und nicht auf ethisch positive Aktionen konzentriert.

Schaffen Sie Geschäftswachstum durch Reputation – mit Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud beseitigt Risiken und ermöglicht es Ihrem Unternehmen, mit Cybersicherheit das Wachstum zu steigern – für eine sichere, rentable und erfolgreiche Zukunft. So wissen Sie nicht nur, dass Ihr Unternehmen durch einen **vielfach ausgezeichneten Cybersicherheitsanbieter** geschützt ist, sondern können dieses Vertrauen auch in Ihre Kommunikation mit Kunden und Stakeholdern einfließen lassen. Dieses Vertrauen schafft ein klares Alleinstellungsmerkmal gegenüber Wettbewerbern, die beim Reputationsbereich Sicherheit hinterherhinken – so wie auch Volvo sich mit seiner mutigen Werbung in den 80ern in Sachen Sicherheit einen Vorsprung vor der Konkurrenz verschaffen konnte.

Kaspersky Endpoint Security Cloud wurde speziell für das Zeitalter von Cloud, Fernzugriff und BYOD entwickelt, löst reale Probleme und lässt sich ganz einfach verwalten. So erhalten Unternehmen, die sich auf Wachstum konzentrieren, leistungsstarke Sicherheit und Kontrolle.

Eine der Technologien, die in der Lösung enthalten sind, ist die NEUE Erkennung von Cloud Services, die Mitarbeiter automatisch daran hindert, nicht autorisierte Cloud Services zu verwenden. So entfällt aufwändiges Micromanagement und Sie müssen sich keine Sorgen mehr darum machen, dass die Vielzahl unzulässiger Services die Sicherheit Ihres Unternehmens gefährden.

Darüber hinaus erhalten Sie mit dem Paket auch Kaspersky Security for Microsoft Office 365, unsere Sicherheitslösung speziell für die gesamte Office-Suite. Diese Komponente ist besonders wichtig, da Microsoft-Produkte nach wie eines der beliebtesten von Cyberkriminellen sind.
Und weil Mitarbeiter heute immer öfter remote arbeiten, erhält jeder Nutzer außerdem zwei kostenlose Lizenzen für mobile Geräte. So erhalten Sie umfassende Cybersicherheit, die sich auf Nutzer und nicht auf Geräte konzentriert. Sie können Richtlinien remote durchsetzen, damit Ihre Mitarbeiter immer geschützt sind – egal, ob sie gerade im Café oder am Strand arbeiten.

Kaspersky Endpoint Security Cloud wird in der Cloud gehostet. Sie benötigen also keine Hard- oder Software und müssen auch nicht für Bereitstellung und Verwaltung bezahlen. Stattdessen erhalten Sie sofortigen Schutz durch vordefinierte Sicherheitsrichtlinien, die von unseren internen Experten entwickelt wurden. Und abgerechnet wird die Lösung über ein flexibles monatliches Abo, um finanzielle Ressourcen freizusetzen.

Für unsere 4000 internationalen Experten **ist Sicherheit wirklich alles**. Sie leben Cybersicherheit, damit Unternehmen auf der ganzen Welt unsere Leidenschaft für das Thema und unsere Auszeichnungen in diesem Bereich für sich nutzen können, um eine sichere Grundlage für die Zukunft aufzubauen.

Sprechen Sie mit uns darüber, wie auch Sie mit **Kaspersky Endpoint Security Cloud** Cyberstolz und eine sichere Reputation aufbauen können, um das Wachstum zu fördern.

Cyber Threat News: https://de.securelist.com/
Neuigkeiten zur IT-Sicherheit: https://www.kaspersky.de/blog/b2b/

www.kaspersky.de

kaspersky BRING ON THE FUTURE