Mehr Cybersicherheit
im digitalen Marketing

Die Bedeutung der Cybersicherheit im digitalen Marketing wächst stetig, denn mit der immer größer werdenden Abhängigkeit von digitalen Systemen steigt auch das Risiko von digitalen Angriffen. In diesem Kontext ist es für Unternehmen vor allem wichtig, die Integrität und Sicherheit von Kundendaten sicherzustellen sowie ihre Markenreputation zu schützen. Doch was können Unternehmen tun, um die digitale Sicherheit zu verbessern?

Was versteht man unter Cybersicherheit?

Digitale Angriffe zielen darauf ab, unerlaubten Zugriff auf Daten zu erlangen, Daten zu ändern oder zu löschen, den normalen Betrieb eines Systems zu stören oder sogar einen Angriff auf ein bestimmtes Ziel durchzuführen. Dem gegenüber steht die Cybersicherheit, auch bekannt als IT-Sicherheit. Ihr Hauptziel ist es, Geräte, Netzwerke oder Daten vor diesen Angriffen zu schützen. Dafür gibt es eine Reihe von Prozessen, Technologien und Maßnahmen, die entwickelt wurden und die in den Bereich der Cybersicherheit eingeordnet werden können.

Welche Unternehmen sind von Cyberangriffen bedroht?

Prinzipiell sind weder öffentliche Einrichtungen noch Unternehmen – unabhängig von ihrer Größe, Branche oder geografischen Lage – vor der Bedrohung durch Cyberangriffe sicher. Tatsächlich sind es gerade kleine und mittlere Unternehmen (KMU), die immer wieder zur Zielschreibe von Cyberkriminellen werden. Das liegt häufig daran, dass sie nicht über die entsprechenden Ressourcen verfügen und somit anfälliger für Cyberangriffe sind.Ein Report von Symantec aus dem Jahr 2019 bestätigt diese Tendenz. Die Studie ergab, dass 43 Prozent der digitalen Angriffe kleine und mittlere Unternehmen betrafen.

Die Gründe hierfür sind vielfältig. Manchmal zählten mittelständische Unternehmen zu den direkten Zielen der Angreifer, da sie seltener in hochklassige Cybersicherheit investieren und einfacher zu infiltrieren sind. Andererseits können KMU auch als Einfallstor zu komplexeren Netzwerken oder größeren Unternehmen dienen, mit denen sie verbunden sind. Großunternehmen und multinationale Konzerne sind aber nicht weniger gefährdet. Aufgrund ihrer Größe und Komplexität haben sie oft mehr potenzielle Schwachstellen. Darüber hinaus verfügen sie über wertvolle Ressourcen und Daten, die für Cyberkriminelle attraktiv sind. Unter dem Strich bedeutet dies, dass das Thema „Cybersicherheit“ jedes Unternehmen betrifft.

Typische Bedrohungen im digitalen Marketing

Die Möglichkeiten von Angreifern sind groß und können in nahezu jedem Unternehmensbereich auftreten. Gerade im digitalen Marketing gibt es aber eine Reihe von spezifischen Cyberbedrohungen:

1. Phishing-Attacken
Diese Art von Angriffen ist dafür bekannt, dass sie über Social-Engineering-Methoden Schaden anrichten. Im digitalen Marketingkontext können Angreifer Phishing-Attacken dazu verwenden, sensible Kundendaten und Unternehmensinformationen zu stehlen. Besonders gerne setzen Kriminelle dafür auf Fake E-Mails, mit denen sie persönliche Informationen sammeln.

2. Malware und Ransomware
Malware ist jedes Stück Software, das dazu entwickelt wurde, einem Computer oder Netzwerk Schaden zuzufügen. Ransomware ist eine spezielle Art von Malware, die dazu verwendet wird, den Zugang zu einem Computersystem oder den darin enthaltenen Daten zu sperren, bis eine Lösegeldforderung erfüllt ist.

3. DDoS-Angriffe (Distributed Denial of Service)
Eine DDoS-Attacke ist ein Versuch, einen Online-Service durch eine Überlastung lahmzulegen. Für digitale Marketingunternehmen kann dies zu erheblichen Geschäftsunterbrechungen und Reputationsschäden führen – insbesondere dann, wenn die Website eines Unternehmens für seine Geschäftstätigkeit zentral ist.

4. Cross-Site Scripting (XSS)
Hierbei werden schädliche Skripte in vertrauenswürdige Websites eingefügt, die dann im Browser des Nutzers ausgeführt werden. Das kann beispielsweise zum Diebstahl von Session-Cookies führen.

5. Man-in-the-Middle-Angriffe (MitM)
Bei dieser Art von Angriff positioniert sich der Angreifer in einer Kommunikation zwischen zwei Parteien. Er kann die Kommunikation abfangen, die übertragenen Daten manipulieren oder eigene Nachrichten einfügen.

Darum ist die digitale Sicherheit wichtig für Unternehmen

Kunden vertrauen darauf, dass Unternehmen ihre persönlichen Informationen sorgfältig und sicher behandeln. Jeglicher Bruch dieses Vertrauens durch Datenschutzverletzungen kann weitreichende Folgen für ein Unternehmen haben. So können sich Kunden etwa entscheiden, die Geschäftsbeziehung zu beenden und sich nach alternativen Partnern umzusehen. Für betroffene Unternehmen kann das enorme finanzielle Schäden nach sich ziehen, die sogar existenzbedrohend werden können.

Darüber hinaus können Angriffe die öffentliche Wahrnehmung und Reputation eines Unternehmens erheblich beeinflussen. Gerade im Hinblick auf das Neukundengeschäft können Sicherheitslücken potenzielle Kunden davon abhalten, Geschäfte mit ihnen abzuschließen.

Auf der anderen Seite kann ein mittelständisches Unternehmen, das in eine solide Cybersicherheitsstrategie investiert und diese umsetzt, mit seinem Engagement für den Schutz persönlicher Daten punkten. Wenn Kunden das Gefühl haben, dass ihre Informationen sicher sind, kann das zu mehr Zufriedenheit, stärkerer Loyalität und letztlich einem verbesserten Markenimage führen. In einer Zeit, in der Datendiebstähle immer häufiger vorkommen, kann dies am Ende einen entscheidenden Wettbewerbsvorteil mit sich bringen. Umso mehr sollten Sie als Unternehmer sich um Ihre digitale Sicherheit bemühen!

Tipps, wie Sie Ihr Unternehmen schützen können

Die Integration von Cybersicherheit in die digitale Marketingstrategie ist ein mehrschichtiger Prozess, der ein gründliches Verständnis der Bedrohungslandschaft, eine detaillierte Risikobewertung und die Implementierung effektiver Präventionsmaßnahmen erfordert. Nachfolgend haben wir neun effektive Tipps und Maßnahmen zusammengefasst.

1. Richtlinien für Cybersicherheit
Entwickeln Sie klare Richtlinien für die Handhabung und Speicherung von Kundendaten. Diese sollte Regeln für Passwörter, den Zugriff auf Informationen und das Teilen von Daten über soziale Medien enthalten.

2. Regelmäßige Schulungen
Bieten Sie regelmäßige Schulungen zur Cybersicherheit an. Damit stellen Sie sicher, dass alle Mitarbeiter über mögliche Bedrohungen und ´Best Practices´ zum Schutz vor diesen Bedrohungen informiert sind.

3. Sicherheitssoftware
Investieren Sie in entsprechende Technologien, um Ihre Kundendaten sicher zu verschlüsseln. Achten Sie außerdem auf die regelmäßige Aktualisierung dieser Softwarelösungen, um gegen die neuesten Bedrohungen gewappnet zu sein.

4. Backups / Wiederherstellung
Implementieren Sie ein gut geplantes Backup-System und haben Sie klare Wiederherstellungspläne für den Fall eines Cyberangriffs. Dies hilft dabei, Datenverluste zu minimieren und nach einem Angriff schnell wieder den normalen Betrieb aufzunehmen.

5. Überwachung / Incident Response
Implementieren Sie Tools zur Überwachung der Netzwerkaktivitäten, um Anomalien zu erkennen und auf Vorfälle schnell reagieren zu können. Eine frühzeitige Erkennung von Angriffen kann die Schadensauswirkungen deutlich minimieren.

6. 2-Faktor-Authentifizierung (2FA)
Einfache Passwörter und ungesicherte Logins sind bekannte Sicherheitslücken. Durch Einführung von 2FA für alle Benutzerkonten können Sie das Risiko von unautorisierten Zugängen deutlich senken.

7. Sicherheit in die Planungsphase
Stellen Sie sicher, dass Cybersicherheitsmaßnahmen von Anfang an in Ihre digitalen Marketingstrategien und -pläne integriert werden. Dies gewährleistet, dass Sicherheit kein nachträglicher Gedanke, sondern von Anfang an eine Priorität ist.

8. Einhaltung des Datenschutzes
Achten Sie darauf, dass Sie mit Ihren Aktivitäten im digitalen Marketing die relevanten Datenschutzgesetze einhalten. Verstöße können nicht nur zu Geldbußen führen, sondern auch das Vertrauen von Kunden untergraben und Ihre Unternehmensreputation schädigen. Schreiben Sie den Datenschutz im Unternehmen deshalb immer groß.

9. Zusammenarbeit mit Profis
Überlegen Sie, externe IT-Sicherheitsberater hinzuzuziehen, die die individuellen Sicherheitsbedürfnisse Ihres Unternehmens verstehen und spezielle Lösungen anbieten können.

Digitale Sicherheit in Zukunft noch wichtiger

Mit der zunehmenden Abhängigkeit von digitalen Technologien steigen auch die damit verbundenen Sicherheitsrisiken. Gerade Technologien wie Künstliche Intelligenz und Big Data eröffnen langfristig neue Möglichkeiten für Cyberangriffe. Das unberechtigte Sammeln und Verwenden von Kundendaten durch fortschrittliche Analysetools kennzeichnet hierbei eine neue Art von Bedrohung, die angegangen werden muss.

Andererseits bieten diese neuen Technologien auch Lösungen zur Verbesserung der Cybersicherheit für Unternehmen. Zum Beispiel kann die Blockchain-Technologie zur Verbesserung der Transparenz und Sicherheit bei der Aufbewahrung und Übertragung von Daten eingesetzt werden.

Während es zwar immer wieder neue Gefahren gibt, werden auf der anderen Seite aber auch neue sicherheitsverbessernde Technologien entwickelt. Unternehmen sind den Cyberkriminellen damit nicht schutzlos ausgeliefert. Allerdings gilt: Wer im digitalen Marketing erfolgreich sein will, muss up to date sein. Wenn Sie die digitale Sicherheit in Ihrem Unternehmen verbessern wollen, sollten Sie sich regelmäßig über aktuelle Risiken und mögliche Lösungsansätze informieren.

Magdalena Lürwer, PresseBox