

„DIGITALER VERTRIEB“ – HYPE ODER AM ENDE NUR DIE HALBE WAHRHEIT?

Bei meinem täglichen Social Monitoring auf Instagram und Facebook sowie in den Feeds relevanter Accounts beobachte ich seit einiger Zeit die zunehmenden Inhalte diverser Dental-labore, die mir auf der Basis einer Kampagne ausgespielt werden. In der Regel handelt es sich um ein Reel (Video) mit hinterlegtem Funnel, durch den sich der Interessierte durchklickt und im Idealfall am Ende seine Kontaktdaten hinterlegt, damit der Werbende mit ihm in Kontakt treten kann. Dieser bekommt den Kunden sozusagen auf dem Silbertablett präsentiert – man wird quasi gerufen, statt Klinken zu putzen. Klingt wie im Schlaraffenland, in dem einem ja bekanntlich die gebratenen Tauben in den Mund fliegen.

Das echte Leben sieht anders aus. Zu einem ganzheitlichen Vertriebsansatz gehört heute selbstverständlich auch eine gut geführte Präsenz auf den digitalen Kanälen dazu. Sie schafft nicht nur Reichweite, Sichtbarkeit und Bekanntheit, sondern steht häufig

auch als Surrogat für Innovationskraft und Modernität im Unternehmen. Ziel dieser Präsenzen ist es, Leads zu generieren, d. h. Vertriebschancen, in unserem Sinne Zahnarztpraxen, die um Kontaktaufnahme bitten. Was will man mehr?

Grundsätzlich ist das Ziel jeder Art von Vertrieb, mit potenziellen Kunden in Kontakt zu kommen, um

diese dann für sich zu gewinnen. Allerdings – und das ist wichtig – ist ein Lead noch lange kein Kunde und ein Gespräch, selbst wenn der potenzielle Kunde es selbst eingefordert hat, macht noch keinen Umsatz. Jeder digital generierte Lead braucht irgendwann menschliche Vertriebskompetenz, also die Fähigkeit, in einem Termin aus dem Lead einen Kunden zu machen und im weiteren Verlauf aus dem Neu- einen umsatzstarken Bestandskunden zu generieren. Digitale Kampagnen liefern hier zu, das tatsächliche Gewinnen funktioniert nur über den persönlichen Kontakt und die Kompetenz, „den Sack zuzumachen“.

Ob Social-Media-Kampagnen ein Erfolg oder ein Fass ohne Boden werden, liegt am hinterlegten Vertriebsprozess: Wie sieht ein vertriebslich sinnvolles erstes Gespräch aus? Was ist das Ziel dieses Gesprächs? Wie könnten notwendige weitere Kontakte aussehen? Was führt sicher zur ersten, was sicher zu vielen weiteren Arbeiten? Wer hier keine Antworten hat und wer die Möglichkeiten auf Social Media nutzt, um nicht selbst „in den Vertrieb“ zu müssen, dessen Ergebnisse bleiben weit unter den Möglichkeiten.

Am Ende ist der erfolgreich, dessen Vertriebsaktivitäten auf den unterschiedlichen Kanälen und mit den unterschiedlichen Vorgehensweisen sinnvoll miteinander verwoben, fein aufeinander abgestimmt und professionell zu Ende gebracht sind.

Denn: Menschen kaufen bei Menschen und wer die Beziehung hat, hat den Kunden. Alles davor ist delegierbares Vorspiel – ohne Struktur und Kompetenz im persönlichen Vertrieb bleibt es aber häufig auch genau das.

Infos zur
Autorin



**Claudia Huhn –
Beratung Coaching
Training**
www.claudiahuhn.de



© privat

Jedes fünfte Ransomware-Opfer hat schon einmal Lösegeld gezahlt

Fast jedes zweite Unternehmen (45 Prozent) war in den vergangenen zwölf Monaten von einem Ransomware-Angriff betroffen, oft werden dabei auch die IT-Systeme der Opfer verschlüsselt und blockiert, wodurch der gesamte Betrieb stillstehen kann. Bei 25 Prozent ist dabei ein Schaden entstanden, bei 20 Prozent blieb der Angriff ohne Folgen. Die große Mehrheit der betroffenen Unternehmen zahlt nicht: 66 Prozent haben den Erpressern nichts überwiesen. Jedes Fünfte (20 Prozent) hat aber schon Lösegeld gezahlt, 14 Prozent wollen oder können dazu keine Angabe machen. Das sind Ergebnisse einer repräsentativen Telefon-Befragung von 1.003 Unternehmen ab zehn Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom.

„Jede Zahlung finanziert den nächsten Angriff. Und selbst wer zahlt, erhält keine Garantie: Weder für die Entschlüsselung seiner Daten noch dafür, dass die Täter die Daten nicht doch veröffentlichen oder weiterverkaufen“, sagt Bitkom-Präsident Dr. Ralf Wintergerst.

Was Unternehmen tun können

Der Bitkom empfiehlt Unternehmen fünf Maßnahmen, um Ransomware-Angriffe abzuwehren und im Ernstfall handlungsfähig zu bleiben:

1. **Die eigene IT-Landschaft kennen.** Wer nicht weiß, welche Systeme, Datenbestände und Schnittstellen im Einsatz sind, hat keine Informationen zur eigenen Verwundbarkeit und kann nach einem Angriff die Be-

troffenheit nicht abschätzen. Eine aktuelle Übersicht über Systeme, Zugänge und Abhängigkeiten ist die Grundlage jeder Reaktion.

2. **Back-ups machen** – und offline halten. Viele Unternehmen haben gar keine oder nur unvollständige Sicherungen ihrer Daten, das spielt Erpressern, die Daten verschlüsseln und den Zugang kontrollieren, in die Hände. Wer Back-ups besitzt, sollte sie vom Netz getrennt aufbewahren, damit sie sich nicht mitverschlüsseln oder stehlen lassen. Und das Zurückspielen gehört regelmäßig geprobt, nicht erst im Schadensfall.

3. **Zugänge absichern.** Die konsequente Nutzung von Mehr-Faktor-Authentifizierung, ein striktes Rechtemanagement und die regelmäßige Löschung nicht mehr benötigter Konten schließen die Einfallstore, die Angreifer am häufigsten nutzen.

4. **Angriffe früh erkennen.** Die unzureichende Erkennung von Sicherheitsvorfällen ist die häufigste Ursache dafür, dass aus einem Angriff ein Schaden wird. Protokolldaten müssen durchgängig ausgewertet und überwacht werden, um schnell reagieren zu können.

5. **Den Notfall üben.** Ein Notfallplan ist ein Muss, und zwar so, dass auf ihn beim Ausfall der IT auch zugegriffen werden kann. Darin müssen Verantwortlichkeiten, Meldewege und vorbereitete Krisenkommunikation enthalten sein. Geübte Abläufe entscheiden über Stunden oder Wochen Stillstand.

Quelle: Bitkom e.V.



© Zaina – stock.adobe.com (KI-generiert)