maz
KOMMUNIKATION

Szenario:
Cyberangriff auf Elektrizitätswerke Rheingau AG

Musterlösung

Disclaimer:
*Musterlösungen zu unseren Szenarien sind immer als **eine Möglichkeit** zu sehen, wie die Krisenlage angegangen werden kann. Unsere Musterlösungen erheben nicht den Anspruch, den alleine glückselig machenden Weg zur einer raschen Bewältigung einer Krise darzustellen.*

Aufgabe 1:

Überlegen Sie das Wording der ersten Stunde

Vorschlag

Unter dem Wording der ersten Stunde verstehen wir die Kernbotschaft, welche der Krisenstab im Sinne einer Sofortmassnahme als eine der ersten Entscheidungen trifft. Das Wording der ersten Stunde dient dazu, widersprüchliche Aussagen gleich zu Beginn einer Krise zu verhindern und alle Involvierten auf eine gemeinsame Sprachregelung «einzuschwören». Was für alle Sofortmassnahmen gilt, gilt auch für das Wording der ersten Stunde: Es darf keine späteren Entscheide des Krisenstabes oder der Krisenkommunikation präjudizieren. Entsprechend muss ein Wording der ersten Stunde meist noch relativ offen und unverbindlich bleiben.

Wichtig beim Wording der ersten Stunde ist, die vorhandenen Informationen gleichsam schon zu verifizieren, bevor sie verwendet werden. Es ist eine Konstante jeder Krisenlage, dass ganz zu Beginn widersprüchliche Informationen vorhanden sind und/oder Gerüchte und Spekulationen ins Kraut schiessen. Die Literatur hat für diese Phase den Begriff «Chaosphase» geprägt. Wenn sich die Krisenkommunikation in dieser Phase Fehler leistet (z.B. indem sie Falschinformationen verbreitet), kann das die spätere Krisenbewältigung wesentlich beeinträchtigen.

Im vorliegenden Szenario könnte ein Wording der ersten Stunde zum Beispiel lauten:

«Die Elektrizitätswerke Rheinbau AG sind heute Opfer eines Hackerangriffs geworden. Betroffen sind nach aktuellem Stand E-Mail-Konten von Kundinnen und Kunden. Die Elektrizitätsversorgung ist nicht betroffen. Wir arbeiten mit Hochdruck daran, das Problem zu lösen.»

Aufgabe 2:

Führen Sie eine allgemeine Problemerfassung durch.

Vorschlag

Wir verwenden für die Problemerfassung das entsprechende Formular der Firma SPINNLER | MEIER | SENN (vgl. Beilage).

Aufgaben aus dem Update

Aufgabe 1

Überlegen Sie, inwiefern die neue Entwicklung Einfluss auf Ihre Handlungen/Botschaften hat. Müssen Sie Ihr Wording ändern? Falls ja, was schlagen Sie dem Krisenstab vor?

Vorschlag

1.) Bei Hacker-Angriffen gilt (wie generell, wenn eine Organisation Opfer von kriminellen Angriffen geworden ist), dass detaillierte Informationen über die Art des Angriffs in der Öffentlichkeit kontraproduktiv sind; derlei sensitive Informationen können anderen Angreifern wertvolle Informationen geben, was nicht in unserem Interesse ist. Deshalb empfiehlt es sich, keine Details über die Art des Angriffes zu offenbaren. Entsprechende Anfragen können wie folgt beantwortet werden:
«Wir möchten keine Details über die Art des Angriffs veröffentlichen, weil wir damit den Angriefern in die Hände spielen könnten, und das wollen wir natürlich nicht - was Ihr Publikum sicher auch versteht.»

2.) Auch was noch unklar ist (3. und 6. Abschnitt der Lageentwicklung), kommunizieren wir nicht. Wir beschränken uns in der Krisenkommunikation auf bestätigte Fakten. Wenn Fragen zu diesen Punkten kommen, kann die Antwort zum Beispiel lauten:
«Diese Fragen werden gegenwärtig von den Experten noch geklärt, wir können dazu keine abschliessenden Aussagen machen.»

3.) Bezüglich der gestohlenen Kundendaten und Passwörter empfiehlt es sich, an die Kund/innen konkrete Handlungsempfehlungen zu geben. Beispielsweise:
«Falls Sie auf Ihr Konto nicht mehr zugreifen können: Loggen Sie sich im Webmail ein und lassen Sie sich auf Ihr Handy oder eine alternative E-Mail-Adresse einen Link zusenden, um ein neues Passwort einzurichten.»

4.) Auch was noch unklar ist (3. und 6. Abschnitt der Lageentwicklung), kommunizieren wir nicht. Wir beschränken uns in der Krisenkommunikation auf bestätigte Fakten. Wenn Fragen zu diesen Punkten kommen, kann die Antwort zum Beispiel lauten:

«Diese Fragen werden gegenwärtig von den Experten noch geklärt, wir können dazu keine abschliessenden Aussagen machen.»

Aufgabe 2

Ihr Verwaltungsratspräsident, Nationalrat Hans Schlüter, möchte testen, ob Sie ausreichend gute Antworten auf kritische Medienfragen hätten und bittet Sie, eine Nasty Questions List zu erstellen und ein Probe-Interview durchzuspielen.

Vorschlag

Sie wurden heute Opfer eines Hacker-Angriffs. Waren Ihre System unzureichend geschützt?

Wir waren bis heute überzeugt, ausreichend geschützt zu sein: Wir befolgen alle Best-Pratice-Regeln, gehen zum Teil deutlich über die Branchenstandards hinaus – und doch wurden wir Opfer. Jetzt heisst es, die Angreifer so rasch als möglich auszuschliessen und dann zu analysieren, mit welchen zusätzlichen Vorkehrungen Angriffe wie der heutige verhindert werden können.

Was wissen Sie schon darüber, wie die Hacker in Ihre Systeme eindringen konnten?

Bitte haben Sie Verständnis dafür, dass wir das nicht in der Öffentlichkeit diskutieren möchten – wir würden damit ja den Angreifern in die Hände spielen. Es geht jetzt um etwas anderes: Zunächst müssen wir zusehen, dass die Kundinnen und Kunden rasch wieder Zugang zu ihren Dienstleistungen haben. Und dann, dass wir analysieren, wie wir solche Vorgänge in Zukunft verhindern können.

Was wurde alles an Daten gestohlen?

Der Umfang des Schadens wird gegenwärtig von unseren Spezialisten evaluiert. Wir raten unseren Kundinnen und Kunden auf jeden Fall, die Passwörter Ihrer E-Mail Konten zu ändern und dabei sichere Passwörter zu verwenden. Wir haben auch entschieden, dass wir umgehend eine 2-Stufen-Autorisierung für alle E-Mailkonten anbieten werden. Das Ziel ist, dass wir das innerhalb eines Monats anbieten können.

Kundinnen und Kunden lieben das allerdings nicht. Es macht die Handhabung sehr viel komplizierter.

Das ist das ständige Dilemma der Datensicherheit. Sicherheit geht fast immer auf Kosten der Benutzerfreundlichkeit. Wir verpflichten die Kundinnen und Kunden deshalb nicht, wir bieten diese Sicherheitstools nur an.

Es heisst, die Randsomware sei über eine Fotodatei auf Mitarbeiter-E-Mails der RAG eingeschleppt worden?

Wie gesagt, wir möchten die genauen Muster des Angriffs nicht öffentlich diskutieren, das würde nur den Angreifern in die Hände spielen. Wir arbeiten zur Zeit mit einem Krisenstab und mit Hochdruck daran, die Probleme zu beheben. Und natürlich analysieren wir dabei auch, welche Vorkehrungen wir treffen müssen, um in Zukunft noch sicherer zu sein.

Ihr Kerngeschäft ist die Elektrizitätsversorgung, Hosting und Internet sind Nebengeschäfte. Sind Sie zu wenig qualifiziert für dieses Geschäft?

Nein, dieser Schluss erscheint mir unfair. Wir verfolgen im Bereich der Internet-Dienstleistungen Best-Pratice-Regeln, also die gleichen Standards, wie sie auch die allergrössten in der Branche haben. Und

solche Attacken kommen ja auch nicht nur bei uns vor, sondern bei vielen, auch den grössten Anbietern. Jetzt geht es darum, aus dem Vorgefallenen zu lernen.

Sie haben heute gesagt, dass die Elektrizitätsversorgung nicht betroffen sei. Wie können Sie da so sicher sein?

Zwei Gründe: Zum einen sind die Systeme der Elektriziätsversorgung vollständig abgekoppelt vom ordentlichen Internet. Sie kommen also über das Netz nicht auf die Systeme der Leitstelle. Zum zweiten haben wir immer noch die Möglichkeit, Schaltungen im Elektrizitätsnetz von Hand auszuführen und das digitale System der Leitstelle ausser Betrieb zu nehmen. Das macht das Management natürlich einiges komplizierter, aber es geht.

Ein Blackout ist ausgeschlossen?

Es gibt nie eine 100%-ige Sicherheit, das wäre blauäugig. Aber ich kann mir kein Szenario vorstellen, bei dem ein Hackerangriff zu einem Blackout in der Elektrizitätsversorgung führen könnte.

Sie Hosten auch Online-Stores von grossen Anbietern, bei denen Kreditkartendaten verarbeitet werden. Müssen die Kundinnen und Kunden dieser Stores damit rechnen, dass diese Daten abgeflossen und missbraucht werden könnten?

Nein, bei der Struktur der online-Shops kann das nach dem aktuellen Stand ausgeschlossen werden.