Whitepaper
Krisenkommunikation bei Cyberangriffen

Strategien zur effektiven Bewahrung von Vertrauen und Glaubwürdigkeit

controllit
Business Continuity Management

Inhalt

Einleitung

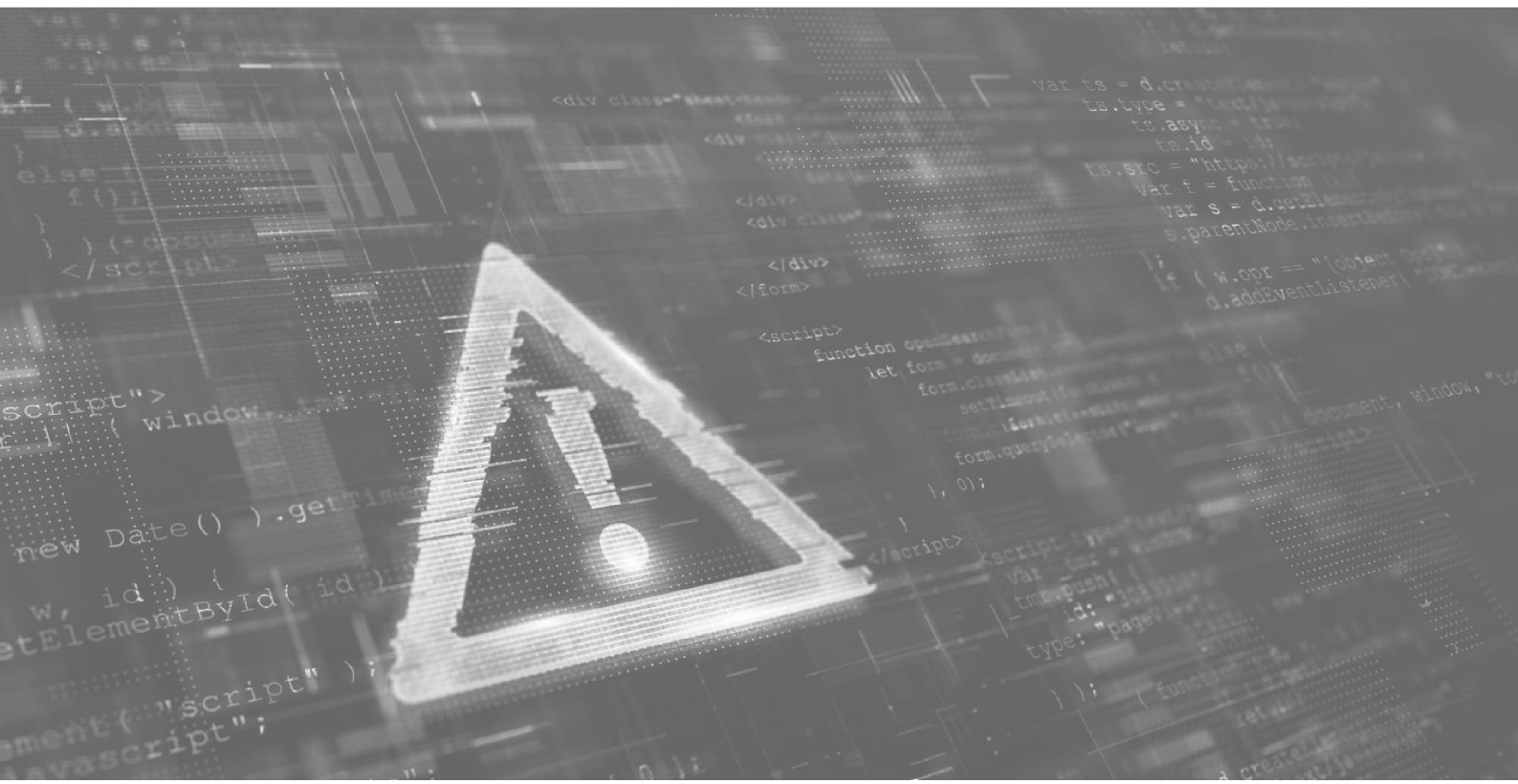
In einer zunehmend digitalisierten Welt sind Unternehmen einem ständigen Risiko von Cyberangriffen ausgesetzt. Die Bewältigung einer solchen Krise erfordert nicht nur technische Maßnahmen, sondern auch eine effektive Krisenkommunikation. Während eines Cyberangriffs spielt die Kommunikation eine entscheidende Rolle, um das Vertrauen der Stakeholder zu bewahren, die Transparenz zu fördern und die Auswirkungen auf das Unternehmen zu minimieren.

Dieses Whitepaper widmet sich der Bedeutung und den Herausforderungen der Krisenkommunikation während eines Cyberangriffs sowie den Strategien, die Unternehmen dabei unterstützen können, diese Herausforderungen erfolgreich zu bewältigen.

Hintergrund und Bedeutung

Die zunehmende Digitalisierung und Vernetzung in der Geschäftswelt bringt zweifellos eine Vielzahl von Vorteilen mit sich. Doch parallel dazu steigt auch die Gefahr von Cyberangriffen rapide an. Die aktuelle Bedrohungslage zeigt deutlich die erhöhte Gefahr von Cyberangriffen auf.

Cyberangriffe auf deutsche Unternehmen nehmen an Häufigkeit und Komplexität zu. Statistiken zeigen, dass diese Angriffe eine ernsthafte Bedrohung für die digitale Sicherheit und die deutsche Wirtschaft darstellen. Keine Branche ist vor Cyberangriffen gefeit. Großkonzerne sind ebenso betroffen wie kleine und mittelständische Unternehmen. Laut einer Studie von Statista aus dem Jahr 2023 sind bereits 58 Prozent der deutschen Unternehmen Opfer von Cyberangriffen geworden. Eine Studie von Bitkom 2023 zeigt zudem, dass bereits 47 Prozent der deutschen Unternehmen auf diesen Trend reagiert und ihre IT-Sicherheitsmaßnahmen verstärkt haben. Globale Krisenherde wie der Angriffskrieg Russlands auf die Ukraine sind dabei zentrale Faktoren, die die Cybersicherheitslage weiter verschärfen.



Hintergrund und Bedeutung

Darüber hinaus haben Cyberangriffe erhebliche finanzielle Auswirkungen auf deutsche Unternehmen. Laut einer Studie von Deloitte aus dem Jahr 2022 belaufen sich die durchschnittlichen Kosten eines Cyberangriffs für ein deutsches Unternehmen auf rund vier Millionen Euro. Diese Kosten umfassen nicht nur direkte Schäden, sondern auch indirekte Ausgaben für Wiederherstellungsmaßnahmen und Reputationsschäden.

Die Bitkom-Studie 2023 beziffert den Gesamtschaden durch Cyberangriffe auf deutsche Unternehmen auf 148,2 Milliarden Euro im Jahr 2023. Krisenkommunikation ist entscheidend für einen erfolgreichen Umgang mit Cyberangriffen. Sie hilft Unternehmen, die finanziellen Folgen zu begrenzen. Zudem stärkt eine effektive Kommunikation gerade in Krisenzeiten das Vertrauen der Stakeholder, was angesichts der Tatsache, dass 58 Prozent der deutschen Unternehmen bereits Opfer solcher Angriffe geworden sind, von großer Bedeutung ist.

Für eine effektive und effiziente Vorbereitung auf Cyberangriffe ist es außerdem notwendig und empfehlenswert, sich mit den Angriffsvektoren von Cyberangriffen und damit dem Vorgehen von Cyberkriminellen auseinanderzusetzen. Cyberkriminelle gehen vielfältig vor, um Unternehmen anzugreifen und zu schwächen. Insbesondere im Rahmen der Krisenkommunikation und den Strategien für die Kommunikation bei einem Cyberangriff ist es von großer Relevanz, sich über die Angriffsvektoren im Klaren zu sein, um Strategien effizient an diese anzupassen. Im Folgenden werden unterschiedliche Arten von Cyberangriffen überblickartig dargestellt.

Angriffsvektoren von Cyberangriffen

Cyberangriffe gibt es in verschiedenster Form - hier einige Beispiele:

Malware wird auf Ihrem Rechner eingerichtet. Hierfür ist eine Handlung seitens des Benutzers erforderlich, z. B. das Anklicken eines Links oder das Öffnen eines E-Mail-Anhangs. Malware kann, sobald sie installiert wurde, vielfältige Schäden anrichten: Blockade von Zugriffen auf zentrale Computersysteme, Verbreitung von weiterer schädlicher Software, Abruf von Informationen durch Datenübergriffe oder Festplatte (Spyware), Unterbrechung des Betriebs von Komponenten, um das System funktionsunfähig zu machen. Bei einem Ransomware-/Malware-Angriff wird eine Lösegeldzahlung von den Angreifern erzwungen.

Bei einem **Phishing-Angriff** sendet der Angreifer betrügerische Nachrichten, z. B. in E-Mails durch Links oder Anhänge. Das Ziel eines Phishing-Angriffs ist es, vertrauliche Daten, wie Kreditkarten- und Anmeldeinformationen, zu stehlen oder Malware zu installieren. Phishing tritt als Cyberbedrohung immer häufiger auf. Diese Art von Angriff kann der erweiterte Angriff gegen einen bestimmten Internetbenutzer sein. Cyberangriffe wie Advanced Persistent Threats (APTs) und Ransomware beginnen häufig mit Phishing.

Eine **Structured Query Language (SQL)-Injection** erfolgt durch schädliche Codes, die der Angreifer in einen Server einfügt, der SQL verwendet. Damit wird der Server gezwungen, Informationen zu zeigen, die er normalerweise nicht zeigen würde. SQL-Injections können durchgeführt werden, indem schädliche Codes in ein anfälliges Suchfeld auf einer Website eingegeben werden.

Angriffsvektoren von Cyberangriffen

Man-in-the-Middle (MitM)-Angriffe nennt man auch Abhörangriffe. Hier schließen sich Angreifer in eine Transaktion zwischen zwei Parteien ein und unterbrechen den Datenverkehr, um Daten zu finden und zu stehlen. Oft führen Angreifer MitM-Angriffe durch folgende Einstiegspunkte durch: öffentliches Wi-Fi-Netzwerke, Malware.

Ein **Denial-of-Service-Angriff** überschwemmt Systeme, Server oder Netzwerke mit Datenverkehr, sodass diese überlasten. Somit ist das System nicht in der Lage, legitime Anfragen zu bearbeiten. Eine DDoS-Attacke wird durch den Versand von Netzwerktraffic durchgeführt. Dieser kann, muss sich aber nicht im Besitz des Angreifers befinden - oft werden Bot-Netzwerke genutzt, die aus Hunderttausenden Computern bestehen. Diese Systeme sind mit Malware infiziert, die einen unbemerkten Fern-zugriff ermöglicht.

Bei einem **Cross-Site Scripting (XSS)** wird ein bösartiger Code auf Web-seiten eingefügt, die dann von nichtsahnenden Benutzern aufgerufen werden. Der Code kann dazu verwendet werden, Daten zu stehlen oder böswillige Aktionen auszuführen. Durch einen Drive-by-Download werden Benutzer dazu verleitet, eine infizierte Website zu besuchen, die dann automatisch Schadsoftware auf ihr Gerät herunterlädt.

Bei einem **Passwort-Angriff** versuchen Angreifer, Passwörter durch Raten, Ausnutzen schwacher Passwörter oder der Anwendung von Brute-Force-/Trial-and-Error-Methoden zu knacken.

Schwachpunkte

Oft sind Mitarbeiter der Schwachpunkt in der Sicherheitsstrategie eines Unternehmens. Laut einer Studie der IBM aus dem Jahr 2023 waren 95 Prozent der erfolgreichen Cyberangriffe auf menschliches Versagen oder Fahrlässigkeit zurückzuführen. Umso bedeutender ist es, eine ganzheitliche Krisenkommunikation aufzubauen und darüber hinaus Mitarbeitern bereits präventiv die Risiken zu kommunizieren oder in akuten Situationen entsprechend Handlungsanweisungen und/oder Sprachregelungen herauszugeben, um sie weiter für die Gefahren von Cyberangriffen zu sensibilisieren. Schulungen und Sensibilisierungsmaßnahmen zum Thema Cybergefahren und Krisenkommunikation für Mitarbeiter sind ein entscheidendes präventives Instrument, um das Risiko von Cyberangriffen zu minimieren und die Krisenkommunikation im Unternehmen zu vereinfachen.

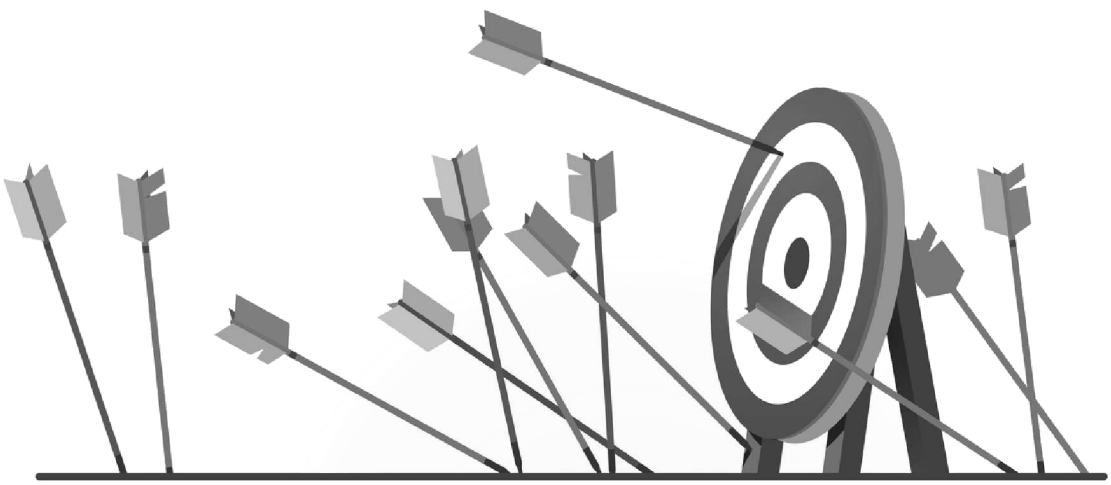
Deutsche Unternehmen sehen sich nicht nur mit den Auswirkungen von Cyberangriffen konfrontiert, sondern auch mit regulatorischen Anforderungen zum Schutz personenbezogener Daten. Verstöße gegen Datenschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO) können zu erheblichen Bußgeldern führen und das Ansehen eines Unternehmens beeinträchtigen.

Insgesamt zeigen diese Statistiken, dass Cyberangriffe eine ernsthafte und wachsende Bedrohung für deutsche Unternehmen darstellen. Es ist unerlässlich, dass Unternehmen proaktiv handeln, um ihre IT-Infrastruktur zu schützen, Mitarbeiter zu schulen und sich den sich ständig verändernden Bedrohungen anzupassen.

Zielsetzung

Dieses White Paper stellt angesichts der steigenden und akuten Gefahrenlage dar, wie Unternehmen kommunikativ während eines Cyberangriffs reagieren können, um die Reputation und das Vertrauen ihrer Stakeholder zu wahren oder wiederherzustellen. Dabei geht es um folgende Punkte:

- **Schnelle Reaktionsfähigkeit sicherstellen:** Entwicklung klar definierter Prozesse und Verfahren für die Krisenkommunikation für den Eintrittsfall eines Cyberangriffs
- **Klare Kommunikationsstrategie entwickeln:** Festlegung von Zielgruppen, Kommunikationskanälen und -inhalten sowie Entwicklung von vorbereiteten Kommunikationsmaterialien, um Stakeholder effektiv zu informieren und zu beruhigen
- **Transparenz und Offenheit fördern:** Förderung einer Kultur der Offenheit mit einer transparenten Kommunikation über den Status des Angriffs, die getroffenen Maßnahmen und die Auswirkungen auf das Unternehmen
- **Schutz des Unternehmensimages und der Reputation:** Entwicklung einer angemessenen sowie rechtzeitigen Reaktion auf negative Berichterstattung und Gerüchte
- **Kontinuierliche Verbesserung und Lernen:** Durchführung von Nachbereitungs- und Evaluationsprozessen, um Stärken und Schwächen während einer Krise zu identifizieren, um Maßnahmen zur Verbesserung zu ergreifen



Herausforderungen der Krisen-kommunikation bei Cyberangriffen

Cyberangriffe stellen für Organisationen jeder Größe und Branche eine ernste Bedrohung dar. Diese Angriffe können rasch zu signifikanten Reputationsschäden führen, insbesondere durch Vertrauensverlust bei wesentlichen Stakeholdern wie Kunden und Lieferanten. Ein solcher Vertrauensverlust kann kaskadenartige Effekte nach sich ziehen und die Markenintegrität der betroffenen Organisationen nachhaltig beeinträchtigen. Der begleitende Einfluss eines Datenlecks während eines Cyberangriffs macht die öffentliche Meinung zu einem entscheidenden Faktor, der die Markenwahrnehmung weiter beschädigen kann.

- **Strukturelle Schwächen in der Kommunikation**

  Eine der größten Herausforderungen ist das Fehlen effizienter Kommunikationsstrukturen, die in Krisenzeiten eine schnelle und kohärente Reaktion ermöglichen. Ohne robuste Mechanismen zur Informationsverbreitung können Unternehmen schwerfällig auf Bedrohungen reagieren, was die Situation oft verschärft.

- **Komplexität und Unvorhersehbarkeit der Cyberbedrohungen**

  Wie Cimbala (2011) anführt, zeichnen sich Cyberangriffe durch eine Vielzahl von Unsicherheiten und Komplexitäten aus, die auf unterschiedlichen Ebenen wirken. Oft bleibt die Identität der Angreifer verborgen, und die Angriffe können intern oder extern, manchmal sogar durch unwissentlich beteiligte Dritte, initiiert werden. Selbst mit fortschrittlichen Sicherheitsmaßnahmen können erfahrene Hacker kontinuierlich und wiederholt angreifen, wobei sie die zunehmende Komplexität und Frequenz von Cyberbedrohungen nutzen. Dies erfordert eine ständige Anpassung und Proaktivität im Cyber-Sicherheitsmanagement.

Herausforderungen der Krisenkommunikation bei Cyberangriffen

- **Dynamische Natur der Cyber-Sicherheitslandschaft**

  Vande Putte und Verhelst (2014) weisen darauf hin, dass die kontinuierlich wandelnde Natur und die zunehmende Raffinesse von Cyberbedrohungen Organisationen zwingen, ihre Sicherheitsstrategien ständig zu überdenken. Die wachsende Abhängigkeit von Informations- und Kommunikationstechnologien macht es schwierig, mit den sich ständig verändernden Bedrohungsszenarien Schritt zu halten. Eine traditionelle Risikoanalyse reicht oft nicht aus, um die Widerstandsfähigkeit von Unternehmen gegenüber modernen Cyberbedrohungen zu stärken.

- **Timing und Inhalt der Krisenkommunikation**

  Die Wahl des richtigen Zeitpunkts und der passenden Kommunikationsinhalte ist entscheidend. Es ist wichtig, die Partner kontinuierlich zu informieren, doch klare Zusagen sind problematisch, da sich die Umstände schnell ändern können.

  Eine vorher definierte Krisenkommunikationsstrategie ist unerlässlich, da sie Unternehmen ermöglicht, bereits im Voraus eine Bedarfsanalyse durchzuführen und umsichtig zu kommunizieren. Zu optimistische Prognosen über eine schnelle Wiederherstellung können zu Frustrationen führen und das Vertrauen der Stakeholder weiter untergraben.

- **Proaktive Kommunikationsvorbereitung**

  Die Vorbereitung auf mögliche Krisenkommunikationsszenarien sollte unmittelbar nach der Mobilisierung der Krisenreaktionseinheit beginnen. Warten, bis der Kommunikationsbedarf entsteht, kann ineffektiv sein, da die Formulierung von Botschaften und die strategische Planung unter Druck zu suboptimalen Ergebnissen führen können.

Diese Herausforderungen verdeutlichen, dass eine effektive Krisenkommunikation während Cyberangriffen nicht nur eine Reaktion auf die Krise selbst ist, sondern auch eine umfassende, vorausschauende Planung erfordert, die die komplexe Natur von Cyberbedrohungen und die Dynamik der öffentlichen Wahrnehmung berücksichtigt.

Strategien für eine effektive Krisen-kommunikation

Welches sind die besten Handlungsoptionen bei einem Cyberangeriff oder Datenverlust? Wenn die Kommunikation zu früh einsetzt, könnten die Angreifer gewarnt werden, während möglicherweise gesichertes Wissen und Fakten über die Situation fehlen. Möglicherweise wird der Vorfall sogar überbewertet, selbst wenn der Schaden schnell eingegrenzt werden kann. Negative Berichterstattung in den Medien ist oft ein hohes Risiko, welches die Krisenkommunikation vermeiden möchte. Im Gegensatz dazu führt eine zu späte Kommunikation zu unvorhersehbaren Ruf- und Haftungsrisiken, während die negative Medienberichterstattung umso umfangreicher sein wird.

Festlegung der Krisenkommunikationsstrategie

Durch die Integration der Situational Crisis Communication Theory von Timothy Coombs sind die drei primären Kommunikationsstrategien 1) Leugnung, 2) Minderung und 3) Wiederaufbaustrategien sowie die sekundäre Stärkungsstrategie besonders wichtig für die Krisenkommunikation während eines Cyberangriffs.

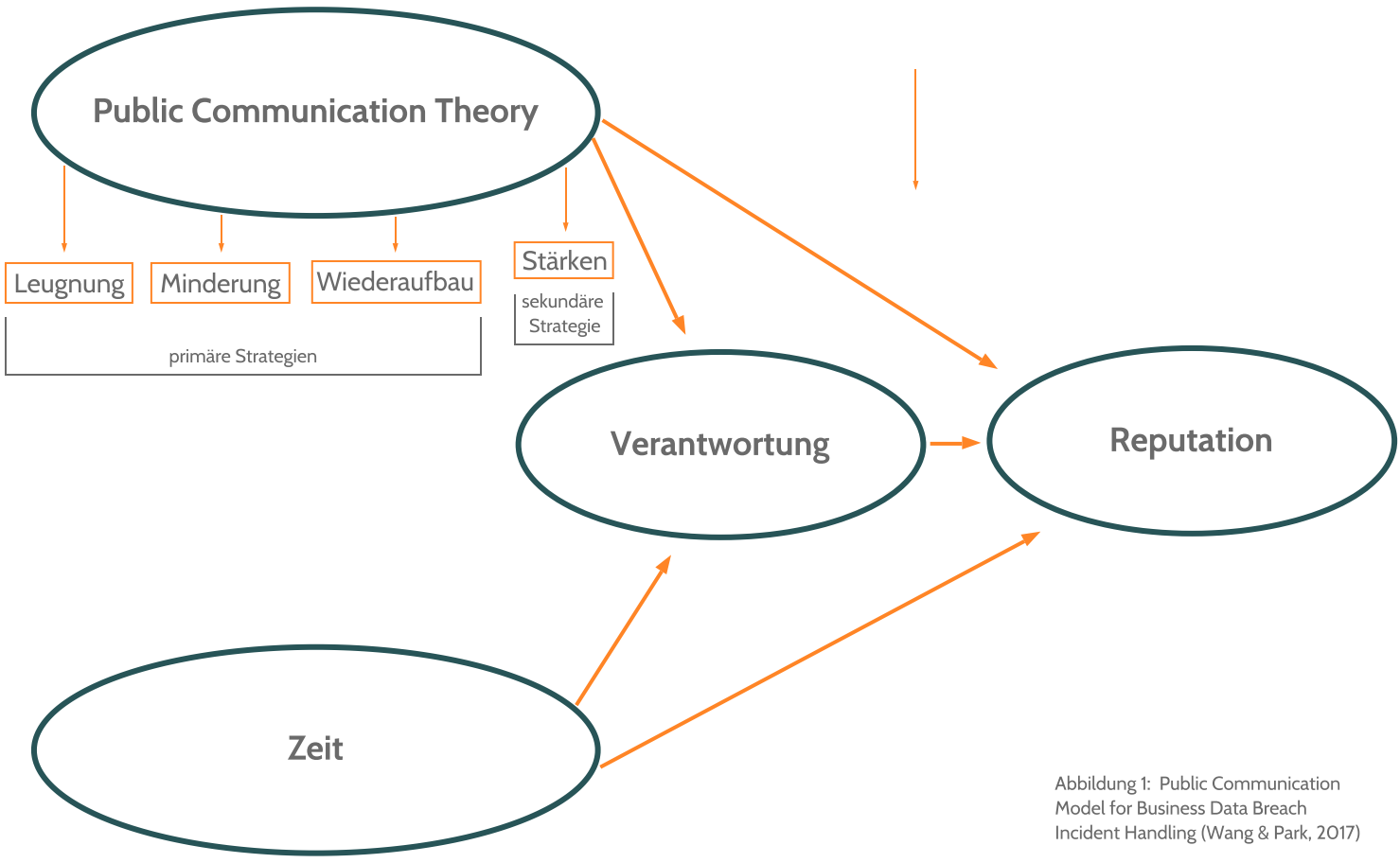


Abbildung 1: Public Communication Model for Business Data Breach Incident Handling (Wang & Park, 2017)

Strategien für eine effektive Krisenkommunikation

Verantwortung und Reputationsmanagement
Ziel einer Krisenkommunikationsstrategie ist es, die Reputation eines Unternehmens zu schützen und zu stärken. Es besteht ein klarer Zusammenhang zwischen der Art und Weise, wie ein Unternehmen mit Vorfällen umgeht, und seiner Reputation. Je stärker die Verantwortung für den Umgang mit Vorfällen wahrgenommen wird, desto höher ist die Reputation des Unternehmens. Die Verantwortung für den Umgang mit Vorfällen wird durch die Art der öffentlichen Kommunikationsstrategien und den Zeitpunkt der Reaktion eines Unternehmens bestimmt (Wang & Park, 2017).

Anpassung Compliance-Anforderungen
Bei der Behandlung von Cybersecurity-Vorfällen ist es besonders wichtig, festgestellte Datenschutzverletzungen gemäß den Compliance-Vorschriften umgehend zu melden und offenzulegen, um rechtliche Strafen und eine negative Wahrnehmung in der Öffentlichkeit zu vermeiden. Die in dem vorgeschlagenen Modell enthaltenen Strategien für die öffentliche Kommunikation sollten sorgfältig im Hinblick auf die Prioritäten und die Leistungsbilanz des Unternehmens geprüft werden, damit sie wirksam zur Schadensbegrenzung bei Cyberangriffen sowie zur Verbesserung des Rufs und der immateriellen Werte eingesetzt werden können.

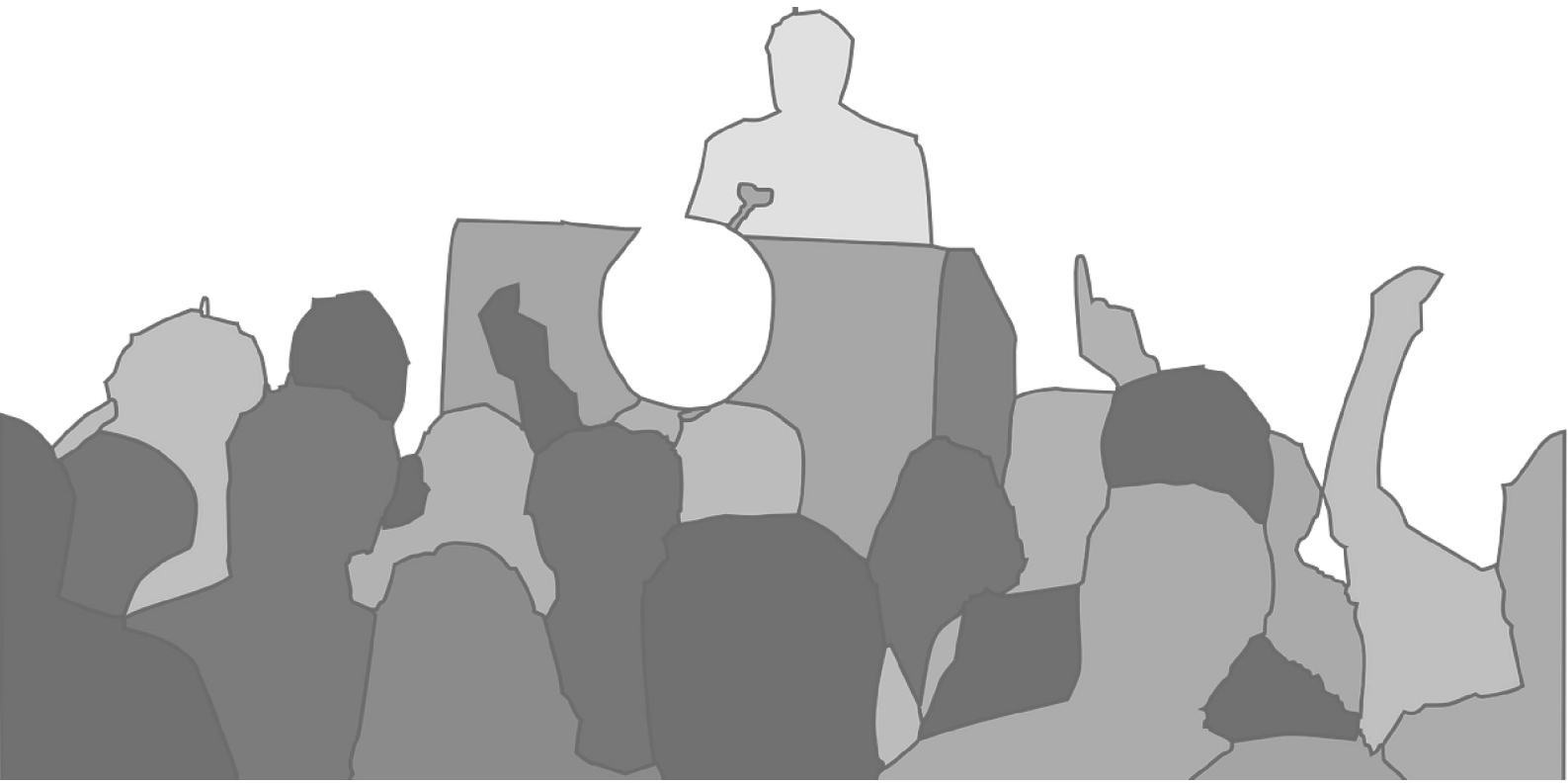
Angesichts der steigenden Nachfrage nach qualifizierten Arbeitskräften für die Cybersecurity sollten Bildungs- und Ausbildungseinrichtungen Kompetenzen und Fähigkeiten im Bereich der öffentlichen Kommunikation in ihre Lehrpläne und Kurse zur Cybersicherheit einbeziehen und betonen. Die Bewertung und Zertifizierung von Cybersicherheitsprogrammen sollte auch die Kompetenz der öffentlichen Kommunikation für die Reaktion auf und den Umgang mit Cyber-Vorfällen widerspiegeln (Wang & Park, 2017).

Schritte für eine effektive Krisenkommunikation

Kommunizieren ja oder nein?
Um die Krisenkommunikation erfolgreich zu bewältigen, ist es unerlässlich, aktiv zu handeln, um sowohl Träger der Botschaften zu sein als auch die Deutungshoheit über diese zu haben. Doch wie und was soll man kommunizieren, wenn man selbst nicht genau weiß, was vor sich geht?

Zunächst geht es nicht darum, detaillierte Informationen zu vermitteln, sondern das Problem anzuerkennen und Verantwortung zu übernehmen Es ist für die betroffenen Stakeholder immer besser, schlechte Nachrichten direkt von dem betroffenen Unternehmen zu erfahren als durch Gerüchte oder Medienberichte.

Die Krisenkommunikation muss außerdem den strategischen Anforderungen bezüglich der operativen Auswirkungen des Cyberangriffs gerecht werden. Dabei geht es nicht nur darum, ob kommuniziert werden soll oder nicht, sondern auch darum, an wen und auf welche Weise kommuniziert werden soll.



Schritte für eine effektive Krisenkommunikation

Wer kommuniziert?
Die Krisenkommunikation muss mit der Kommunikationsstrategie des Unternehmens in Einklang stehen. Interne und externe Kommunikation ist grundlegend und beinhaltet je nach Unternehmen vielfältige und unterschiedliche Stakeholder, die adressiert werden müssen. Es gilt, diese mithilfe einer Stakeholder-Analyse bereits im Vorfeld zu identifizieren. In diesem Zusammenhang ist es auch relevant, die Betroffenheit der Stakeholder bei einem Cyberangriff auf das Unternehmen zu definieren. Folgende Stakeholder sollten bei einem Cyberangriff auf jeden Fall in die Krisenkommunikation eingebunden werden.

- **Mitarbeiter:** Es ist entscheidend, Mitarbeiter nicht nur kontinuierlich über den aktuellen Stand zu informieren, sondern auch darüber, wie ein Cyberangriff ihre Arbeitsabläufe beeinträchtigt, welche Alternativlösungen möglich sind und wie lange die Beeinträchtigung voraussichtlich dauern wird. Darüber hinaus ist es von großer Bedeutung, sie mit Handlungsempfehlungen zur Vermeidung weiterer Sicherheitslücken zu versorgen und mit klaren Kommunikationsrichtlinien auszustatten, da sie oft als Sprachrohr nach außen dienen.

- **Kunden:** Kunden stellen eine weitere wesentliche Stakeholdergruppe dar. Insbesondere bei einem Cyberangriff auf das Unternehmen sind sie oft unmittelbar betroffen. Daher ist es ratsam, sie kontinuierlich mit aktuellen Informationen über die Situation, getroffene Maßnahmen zur Bewältigung und alle relevanten Details zu versorgen.

- **Behörden/Polizei:** Behörden spielen eine entscheidende Rolle bei der Meldung von Cyberangriffen und sollten unbedingt in die Krisenkommunikation einbezogen werden, um Strafzahlungen zu vermeiden. Zudem ist die Zusammenarbeit mit der Polizei bei einem Cyberangriff von zentraler Bedeutung, um die Strafverfolgung der Angreifer einzuleiten und weitere Schäden oder Angriffe gemeinsam zu verhindern.

- **Medien:** Die Medien stellen stets eine der wichtigsten Stakeholdergruppen dar. Ziel ist es, insbesondere in der Kommunikation mit den Medien die Deutungshoheit zu behalten, die Reputation nach außen zu wahren und Transparenz zu zeigen.

Schritte für eine effektive Krisenkommunikation

Nachdem alle Stakeholder identifiziert wurden, sind diese für eine effektive Krisenkommunikation entsprechend ihren Interessen und Einflüssen zu priorisieren. Dabei sind, wie oben bereits beschrieben, unterschiedlichste Stakeholder zu betrachten, wie beispielsweise Kunden, Partner, Mitarbeiter, Aufsichtsbehörden, Medien, Investoren, Lieferanten, Wettbewerber und andere. Es ist wesentlich, ihre Bedürfnisse, Erwartungen und Bedenken zu verstehen und die Kommunikation entsprechend anzupassen. Zum Beispiel möchten Ihre Kunden möglicherweise wissen, wie sich ein Angriff auf Ihre Daten und Dienste auswirkt, während Ihre Mitarbeiter Informationen benötigen könnten, um angemessen zu reagieren und bei der Wiederherstellung zu unterstützen. Ihre Aufsichtsbehörden wiederum möchten möglicherweise darüber informiert werden, wie Sie die geltenden Gesetze und Standards einhalten.

Nachdem schließlich die Stakeholder und deren Bedürfnisse identifiziert wurden, ist es wichtig, die geeigneten Kommunikationskanäle auszuwählen. Je nach Situation können verschiedene Kanäle wie E-Mail, Telefon, soziale Medien, Websites, Pressemitteilungen, Webinare oder persönliche Treffen genutzt werden. Dabei müssen die Vor- und Nachteile der einzelnen Kanäle berücksichtigt werden, wie beispielsweise Geschwindigkeit, Reichweite, Kosten, Interaktivität und Glaubwürdigkeit. Zudem ist eine Koordination der Kanäle erforderlich, um Konsistenz und Genauigkeit sicherzustellen.

Schritte für eine effektive Krisenkommunikation

Bei der Übermittlung Ihrer Nachrichten während eines Cyberangriffs ist es wichtig, bewährte Praktiken zu befolgen. Sie sollten transparent und ehrlich darüber informieren, was geschehen ist, welche Maßnahmen ergriffen werden und was erwartet wird. Gleichzeitig ist es wichtig, einfühlsam und respektvoll gegenüber den Stakeholdern zu sein, ihre Gefühle und Frustrationen anzuerkennen und proaktiv sowie zeitnah Updates und Feedback bereitzustellen. Technische Aspekte sollten klar und prägnant erklärt werden, wobei auf die Vermeidung von Fachjargon und Akronyme geachtet werden sollte. Zudem ist es wichtig, positiv und selbstbewusst zu kommunizieren, um das Engagement und die Fähigkeit zur Bewältigung der Krise zu betonen.

Wie wird kommuniziert?
Das Schlüsselwort ist Konsistenz. Informationslücken zwischen Abteilungen, die sich innerhalb des Unternehmens oder unter den Stakeholdern ausbreiten könnten, sind ein Anzeichen für Vertrauensverluste. Wem soll man glauben, wenn widersprüchliche Argumente vorgebracht werden? Die Informationen müssen nicht unbedingt falsch sein, sie können auch einfach veraltet sein.

Es ist wichtig, die Erstellung und Verbreitung von Nachrichten, Sprachregelungen und Argumenten im Krisenstab zu zentralisieren. Grundlegend ist auch, den Prozess der Kommunikationsvalidierung zu beherrschen, um zu vermeiden, dass wertvolle Zeit verloren geht.

Transparenz stellt das essenzielle Fundament jeder Krisenkommunikation dar, welches unverzichtbar ist, um das Vertrauen der betroffenen Stakeholder zu bewahren oder wiederherzustellen. Unternehmen sollten präzise Informationen kommunizieren über:

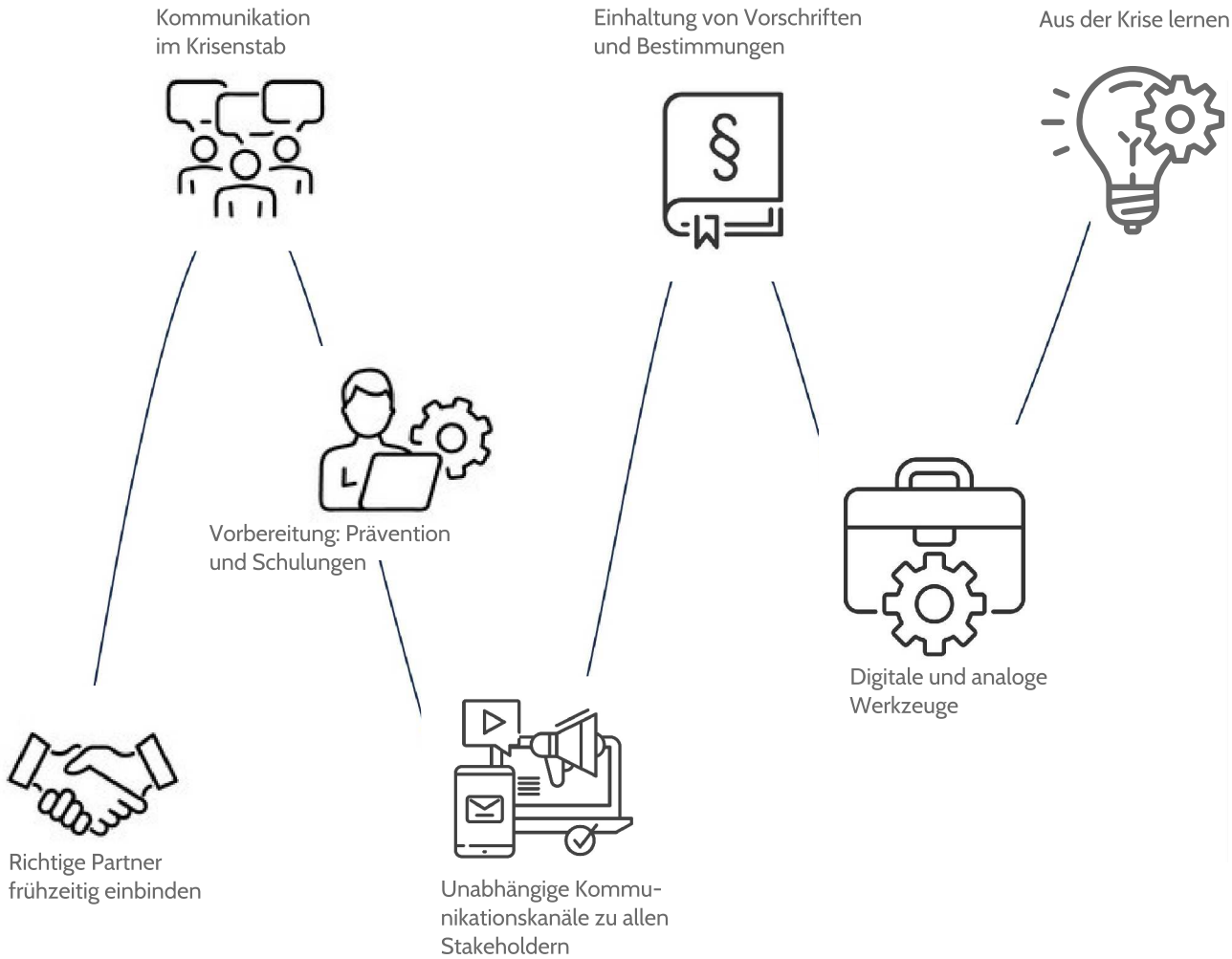
- Art und Herkunft der Kompromittierung
- Ausmaß und die Schwere
- betroffene Daten und Systeme
- potenzielle kurz-, mittel- und langfristige Auswirkungen

Jedoch gilt es, vorsichtig zu sein und im Krisenstab abzuwägen, welche Informationen weitergegeben werden sollen. Es ist deshalb ratsam, den Fokus zunächst auf die Auswirkungen und die schrittweise Wiederherstellung der Dienste zu legen, anstatt sich auf die genauen Ursachen zu konzentrieren, die den Angriff ermöglicht haben. Dies sollte im Nachhinein ausführlich analysiert werden.

Schritte für eine effektive Krisenkommunikation

Wann wird kommuniziert?
Die Kommunikationsstrategie für Cyberangriffe muss in einen Zeitrahmen eingebettet werden. Es kann manchmal Tage oder sogar Wochen dauern, bis das Ausmaß des Angriffs vollständig erfasst ist. Ist das Angriffsmuster erst einmal bekannt, erweist sich der Wiederaufbau des Informationssystems oft als lang andauernde und komplizierte Aufgabe. Oft werden dann Wiederherstellungsfristen verschoben.

Zusammenfassend sind eine Vielzahl von Faktoren bei der Krisenkommunikation während eines Cyberangriffs zu beachten. Hierbei spielen die proaktive Vorbereitung und die aktive Reaktion gleichermaßen wichtige Rollen und sollten entsprechend beachtet werden. Abbildung 2 zeigt zusammenfassend, welche proaktiven und reaktiven Schritte von Relevanz sind, wenn Unternehmen während eines Cyberangriffs erfolgreich kommunizieren wollen.



Key Performance Indicators (KPIs) Krisenkommunikation vs. Cyberangriff

Um den Erfolg der Krisenkommunikation nach den im obigen Kapitel genannten Vorgaben zu messen, ist es sinnvoll, Key Performance Indicators (KPIs) für die Krisenkommunikation bei einem Cyberangriff zu formulieren. Dies ist hilfreich, um in der Nacharbeitung der Krise den Erfolg der Kommunikation zu messen und gezielt Verbesserungspotenziale zu identifizieren. Konkrete qualitative Messgrößen für KPIs in der Krisenkommunikation:

- **Zeitpunkt der ersten Informationsveröffentlichung:** Wie schnell wurde nach der Entdeckung des Cyberangriffs eine offizielle Mitteilung veröffentlicht? Dieser KPI misst die Reaktionszeit und wird in Stunden oder Tagen angegeben.
- **Kontinuität der Informationsverbreitung:** Wurde kontinuierlich und konsistent über den Vorfall und die Fortschritte informiert? Dieser KPI misst, wie regelmäßig Updates veröffentlicht wurden.
- **Richtigkeit der Informationen:** Wurden gesicherte Informationen veröffentlicht oder kam es zu Fehlinformationen? Dieser KPI überprüft die Genauigkeit und Transparenz der bereitgestellten Informationen.
- **Stakeholder-Engagement:** Wie gut wurden Stakeholder eingebunden? Dieser KPI misst, ob alle relevanten Stakeholder rechtzeitig und umfassend informiert wurden, z. B. durch eine Stakeholderanalyse.
- **Einhaltung gesetzlicher Vorschriften:** Wurde der Vorfall rechtzeitig an die Behörden gemeldet und wurden alle relevanten Compliance-Vorgaben eingehalten? Dieser KPI misst, ob gesetzliche Fristen und Vorschriften eingehalten wurden.
- **Nutzer- und Kundenfeedback:** Wie wurde die Krisenkommunikation von Kunden und Mitarbeitern bewertet? Dies kann durch Umfragen oder die Analyse von Social-Media-Kommentaren gemessen werden.
- **Medienmonitoring:** Wie hat sich die Berichterstattung über den Cyber-Angriff entwickelt? Wurde das Narrativ erfolgreich gesteuert oder gab es unerwartet negative Berichterstattung?
- **Vertrauensindex:** Wurde das Vertrauen der Stakeholder in das Unternehmen durch die Krisenkommunikation gestärkt oder geschwächt? Dieser KPI misst die Wirkung der Kommunikation auf die Markenreputation und kann durch externe Reputationsanalysen ermittelt werden.

Zusammenfassung

Dieses Whitepaper beleuchtet die entscheidende Rolle einer gut vorbereiteten Krisenkommunikation im Falle eines Cyberangriffs. Es zeigt auf, dass nicht nur technische Lösungen, sondern auch klare, durchdachte Kommunikationsstrategien notwendig sind, um den Schaden zu begrenzen und das Vertrauen der Stakeholder zu wahren.

Key Takeaways:

- **Vorbereitung ist entscheidend:** Unternehmen sollten bereits im Vorfeld eine Krisenkommunikationsstrategie entwickeln, um im Ernstfall schnell und koordiniert reagieren zu können. Dazu gehört auch, die entsprechenden Verantwortlichkeiten für die Kommunikation festgelegt zu haben.
- **Konsistente und transparente Kommunikation:** Regelmäßige und genaue Informationen sind entscheidend, um das Vertrauen der Stakeholder zu bewahren.
- **Rolle der Stakeholder:** Die frühzeitige Einbindung relevanter Stakeholder, wie Mitarbeiter, Kunden und Behörden, ist von zentraler Bedeutung. Eine Stakeholder-Analyse hilft, die relevanten Interessensgruppen zu identifizieren und die Kommunikationsstrategie entsprechend anzupassen.
- **Medienmonitoring:** Durch ein aktives Monitoring der Berichterstattung und der sozialen Medien können Unternehmen die Kontrolle über das Narrativ behalten und Reputationsschäden minimieren.
- **Lernprozess nach der Krise:** Nach einem Vorfall sollten Unternehmen ihre Strategien evaluieren und Anpassungen vornehmen, um zukünftige Angriffe noch besser bewältigen zu können.

Während Unternehmen immer mehr Bedrohungen durch Cyberangriffe ausgesetzt sind, bieten diese Erkenntnisse einen Leitfaden, um kommunikativ vorbereitet zu sein und den Ernstfall effektiv zu meistern.

Sie haben Fragen zum Thema? Melden Sie sich gern bei uns!

Literatur

https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/#overview

https://www.bitkom.org/Presse/Presseinformation/Bilanz-Cyberkriminalitaet-7-von-10-betroffen

https://www.unibw.de/insurance/reader_2020_cyber_risiken.pdf#page=31

https://iacis.org/iis/2017/2_iis_2017_136-147.pdf

https://www.orangecyberdefense.com/global/blog/cybersecurity/how-to-communicate-in-the-event-of-a-cyberattack

https://www.jcsronline.com/wp-content/uploads/2019/02/Volume-2-Issue-7-Paper-1_new.pdf

https://fleishmanhillard.de/2021/12/the-ten-golden-rules-of-cyber-crisis-communication/?lang=en

https://www.cisco.com/c/de_de/products/security/common-cyberattacks.html

https://www.lintemeier-advisors.com/wp-content/uploads/2021/03/Unternehmenskrisen-und-Stakeholder-Beziehungen-optimiert.pdf

https://www.newsaktuell.de/blog/cybersecurity-und-die-rolle-der-kommunikation

Controllit AG
Kühnehöfe 20
22761 Hamburg
Deutschland
www.controll-it.de

Stand: September 2024

Die Controllit AG ist Ihr Partner für Business Continuity Management (BCM). Seit unserer Gründung entwickeln wir integrative Konzepte und Produkte für das Business Continuity Management, IT Service Continuity Management, Information Security Management und Krisenmanagement. Wir helfen Ihnen mit strategischen, organisatorischen und technischen Konzepten, Ihre Geschäftsprozesse gegen Bedrohungen abzusichern und für Notfälle vorzusorgen.

Foto-/Grafiknachweise: S. 3: iStock.com/Aleksei Naumov; S. 4: iStock.com/Sashkinw; S. 5: iStock.com/SonerCdem; S. 9: iStock.com/IconicBestiary; S. 10: iStock.com/PeopleImages; S. 11: iStock.com/linconvidal; S. 18: iStock.com/Misha Shutkevych, iStock.com/Yuriy Altukhov, iStock.com/Connect, iStock.com/bananajazz