CYBERANGRIFF NOTFALLPLAN

IT & Wirtschaftsinformatik

CAMPUS 02 FACHHOCHSCHULE DER WIRTSCHAFT

Graz, 2024

Impressum

Endbericht

Projekt gefördert durch

DIH SÜD GmbH
Leonhardstraße 59
8010 Graz
https://www.dih-sued.at/

Projekt durchgeführt von

CAMPUS 02
Fachhochschule der Wirtschaft
Department IT & Wirtschaftsinformatik
Körblergasse 126
8010 Graz
https://www.campus02.at/

Autor*innen:
Katharina Moitzi
Angelika Höber
Harris Gerzic
Yevheniia Andriichenko
Stefanie Hatzl

Zitiervorschlag: Moitzi, K., Höber, A., Gerzic, H., Andriichenko, Y., Hatzl, S. (2024). Cyberangriff Notfallplan, Endbericht. CAMPUS 02 Fachhochschule der Wirtschaft.

Disclaimer

Der Leitfaden wurde im Rahmen der DIH-Süd Kooperation gefördert und hat zum Ziel KMUs eine Hilfestellung in der Bewusstseinsbildung im Bereich Cyberkriminalität zu geben. Das Konzept des Leitfadens basiert einerseits auf durchgeführten Interviews mit Expert*innen und/oder betroffenen Unternehmen und andererseits auf bestehenden Leitfäden von professionellen Stellen und Organisationen (z.B. BSI, WKO, etc.). Die Intention des Leitfadens ist es, ausgehend von den Erfahrungen betreffender Unternehmen die Aufmerksamkeit und Dringlichkeit der Thematik zu vermitteln und dadurch Interesse für eine Maßnahmensetzung zu schaffen.

Dieser Leitfaden bietet wertvolle Informationen und Empfehlungen zu Verhaltensweisen bzw. organisatorischen Aspekten im Falle eines Cyberangriffs. Die vorgestellten Maßnahmen und Ratschläge sind als allgemeine Leitlinien gedacht und sollten an die individuelle Situation und die spezifischen Bedürfnisse angepasst werden. Das heißt das vorrangige Ziel ist es Bewusstsein zu schaffen und erste Überlegungen anzustellen, was auf das Unternehmen und dessen Mitarbeiter*innen organisatorisch zukommt in der Situation eines Cyberangriffs. Der Leitfaden ist damit zusätzlich zu einem technischen Sicherheitskonzept zu sehen und ist alleinig keine Garantie für eine rasche und sichere Wiederherstellung und Wiederaufnahme des täglichen Betriebs.

Darüber hinaus ist zu beachten, dass sich Technologien ständig weiterentwickeln und neue Bedrohungen entstehen können. Es ist daher ratsam, regelmäßig den aktuellen Stand der digitalen Infrastruktur zu prüfen und gegebenenfalls Anpassungen an den eigenen Sicherheitsvorkehrungen vorzunehmen.

Die Autor*innen und Herausgeber*innen dieses Leitfadens übernehmen keine Haftung für etwaige Schäden oder Verluste, die durch die Umsetzung der darin enthaltenen Informationen entstehen könnten. Die Verwendung dieser Empfehlungen erfolgt auf eigene Verantwortung. Es wird dringend empfohlen, im Angriffsfall professionelle Beratung und Unterstützung in Anspruch zu nehmen, insbesondere bei komplexen oder schwerwiegenden Sicherheitsfragen. Letztlich liegt es in der Verantwortung des Unternehmens, angemessene Maßnahmen zum Schutz der eigenen IT-Infrastruktur und Daten zu ergreifen. Hierzu empfehlen wir professionelle Dienstleister hinzuzuziehen.

Danksagung

Wir bedanken uns bei allen Personen, die ihre Erfahrungen während und nach eines Cyber-Angriffs mit uns offen und ausführlich geteilt haben. Ein Dank gilt aber auch allen Expert*innen, die ihr Wissen mit uns teilten, sowie allen Organisationen für die Entwicklung frei zugänglicher Leitfäden.

Inhalt

Vorwort

In der heutigen vernetzten Welt ist es unumgänglich, dass wir uns mit dem Thema Cybersecurity auseinandersetzen. Die digitale Landschaft, die wir täglich nutzen, bringt sowohl Chancen als auch Risiken. Cyberangriffe sind keine Hypothesen mehr, sondern eine Realität, der wir uns stellen müssen. In einer Studie von KPMG (2023)[1] wurden Unternehmen befragt, ob sie in den letzten 12 Monaten einen Versuch eines Cyberangriffs feststellen konnten. Alle befragten Unternehmen haben diese Frage mit „Ja“ beantwortet.

Es geht nicht mehr darum, ob man Opfer eines Cyberangriffs wird, sondern vielmehr, wann dieser Fall eintritt.

Trotz dieser Herausforderungen ist es wichtig zu betonen, dass wir nicht hilflos sind. Durch bewusste Vorbereitung, Kenntnis über potenzielle Bedrohungen und eine proaktive Herangehensweise können wir das Risiko eines solchen Angriffs minimieren und seine Auswirkungen eindämmen.

Viele Unternehmen glauben, sie seien nicht von Cyberangriffen betroffen oder es würde sie nie treffen. Doch das kann heutzutage jedem passieren. Oft verlassen sich Unternehmen darauf, dass ihre Daten verschlüsselt und somit sicher sind. Hier setzt jedoch das Konzept "*Harvest now, decrypt later*" an. Betrüger sammeln heute verschlüsselte Daten, um sie später mit fortschrittlicher Technologie zu entschlüsseln. Daher darf man sich nicht allein auf Verschlüsselung verlassen, Cybersecurity umfasst heutzutage viel mehr!

In Momenten eines Cyberangriffs ist es von entscheidender Bedeutung, Ruhe zu bewahren und besonnen zu handeln. Panik kann zu Fehlentscheidungen führen und die Situation verschlimmern. Unser Leitfaden bereitet Sie darauf vor, ruhig und methodisch auf den Angriff zu reagieren. Wir bieten Ihnen einen Überblick über bewährte Strategien und praktische Schritte, um die Auswirkungen des Angriffs zu minimieren und die Sicherheit Ihrer Systeme wiederherzustellen.

Cyberangriffe sind meist kein Versagen einzelner Personen – deshalb ist ein Empowerment aller Beteiligten während der Bewältigung entscheidend

Es ist wichtig anzuerkennen, dass Cyberangriffe oft kein Versagen einzelner Personen sind. In einer zunehmend vernetzten Welt sind wir alle potenzielle Ziele für Cyberkriminalität. Deshalb sollte keine Scham oder Schuldzuweisung einzelner Personen stattfinden. Legen Sie Ihren Fokus darauf, gemeinsam als Team zu handeln, um die Situation zu bewältigen und aus Fehlern zu lernen. Unsere Anleitung bietet Unterstützung und Empowerment für alle Beteiligten, unabhängig von ihrer Rolle oder Position in der Organisation.

Wir laden Sie ein, diesen Leitfaden sorgfältig zu lesen und seine Empfehlungen ernst zu nehmen. Gemeinsam können wir uns besser vorbereiten und widerstandsfähiger gegenüber den Bedrohungen des digitalen Zeitalters werden.

[1] https://de.statista.com/statistik/daten/studie/552445/umfrage/erfahrungen-von-oesterreichischen-unternehmen-mit-cyber-angriffen/ - abgerufen am 25.4.2024

Nichts geht mehr –
die Geschichte eines Cyber-Angriffs

Wie sich ein Cyber-Angriff auch in Ihrem Unternehmen abspielen könnte ...

Mario (38, IT-Mitarbeiter) bekommt am Samstag in der Früh einen Anruf. Er hat dieses Wochenende Bereitschaft. Im Moment arbeitet nur die Schicht-Produktion, somit streikt vermutlich nur wieder einmal der Etiketten-Drucker. „Das ist sicher schnell erledigt" denkt sich Mario und hebt ab. Doch es kommt anders. Thomas, ein Produktionsmitarbeiter, meldet, dass sich die Auftragsdaten für den nächsten Prozessschritt nicht öffnen lassen. Mario möchte sich daraufhin auf den Rechner remote verbinden, um sich das näher anzusehen, aber die Verbindung funktioniert nicht. Er versucht seine Kollegin Clara anzurufen, vielleicht funktioniert es bei ihr, aber er kann sie nicht erreichen. Mario fährt somit in die Firma, um sich das Problem vor Ort anzusehen.

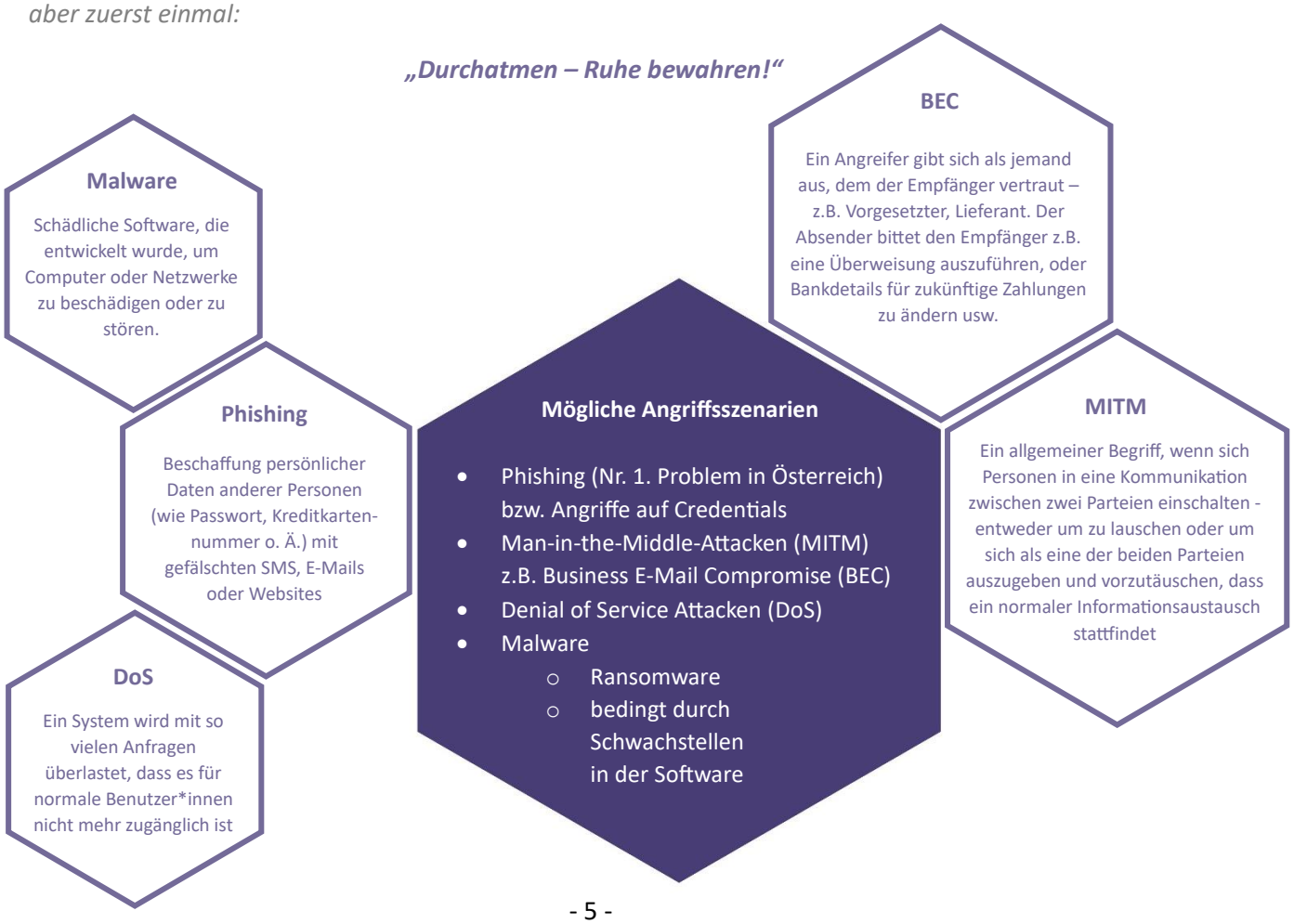
„You're fucked up"

so die Schreckensnachricht, als er sich im Büro am Server einloggen möchte. Das Adrenalin fährt durch den Körper, der Puls steigt, erste Panik kommt auf. Sichtlich nervös geht er zum Regal und sucht den ausgedruckten Notfallleitfaden heraus:

„Shit happens – aber wir sind vorbereitet!

Mario schlägt die Mappe auf und versucht den ersten Rat zu beherzigen. Auch wenn es ihm schwerfällt, aber zuerst einmal:

„Durchatmen – Ruhe bewahren!"



Wie können wir uns vorbereiten?

Die EiLand GmbH ist ein Vorzeigeunternehmen in der Lebensmittelindustrie. Tag für Tag versorgt es die Kundschaft mit frischen, hochwertigen Eiern und dessen Verarbeitungsprodukten. Täglich kommen Lieferwagen mit frischen Eiern an und werden von den EiLand-Logistikteams eingelagert. Das ausgeklügelte Lagersystem ist das Herzstück des Betriebs: vollautomatisiert, durch Software gesteuert und von Robotern und Geräten bedient, die geschickt zwischen den Regalen und Ebenen manövrieren. Am Tag X steht EiLand still: „You're fucked up". Doch draußen dreht sich die Welt weiter: LKWs mit frischen Eiern stehen vor der Tür und niemand weiß, wo diese abgelegt werden können. Der Roboter kann nicht angesteuert werden. Leere LKWs wollen Waren abholen und zur Kundschaft liefern. Auch hier, niemand weiß, welche Eier raus müssen und welche noch liegen bleiben können. Geschweige denn, wie an diese ranzukommen ist. Im Betrieb herrscht Chaos.

Zentrale Geschäftsprozesse absichern

Damit Sie als Unternehmen im Angriffsfall handlungsfähig bleiben, müssen Sie Ihre **kritischen Geschäftsprozesse schützen**. Dazu müssen Sie diese im Vorfeld identifizieren. Zur Identifikation können Sie entweder von Ihren Systemen oder von Ihren Prozessen ausgehen.

Systeme als Ausgangspunkt

Dazu müssen sie erst eine Liste aller IT-bezogenen Komponenten im Unternehmen erstellen (das können IT-Systeme sein, Software, Lizenzen, Infrastruktur, Informationen, …). Anschließend gilt es zu entscheiden, welche am wichtigsten sind und den größten Schutz brauchen. Dabei können folgende Überlegungen helfen:

- „Wie lange kann das Unternehmen ohne das betreffende IT-System, die betreffenden Daten, […] etc. überleben? Wie schnell müssen diese Werte wieder verfügbar sein, um ernsthafte Schäden zu vermeiden?"
- „Welcher Schaden entsteht, wenn die betreffenden Daten in die Hände eines Konkurrenzunternehmens fallen […]?
- "Welche Probleme sind zu erwarten, wenn bestimmte Informationen öffentlich werden […]?"
- „Welcher Schaden entsteht, wenn z.B. die Buchhaltung oder die Kundendatenbank […] aufgrund eines Virenangriffs falsche Einträge enthält?"

Auf diesem Weg kann festgelegt werden, welche Komponenten hohe Schutzmaßnahmen erfordern und wo schwächerer Schutz ausreichen sollte.

Prozesse als Ausgangspunkt

Eine Alternative ist es, ausgehend von den zentralen Geschäftsprozessen strukturiert Schutzmaßnahmen zu definieren und umzusetzen. Dies kann mittels einer Business Impact Analyse (BIA) erfolgen, die - vereinfacht – wie folgt abläuft:

- Kritische Geschäftsprozesse identifizieren.
- Mögliche Schäden abschätzen (wenn der Geschäftsprozess unterbrochen wird).
- Einschätzen: Wie lange kann der Ausfall getragen werden, wie schnell muss der Prozess wiederhergestellt werden können?
- Notfallpläne und Wiederherstellungsstrategien entwickeln.

Arbeitsblatt *Geschäftsprozesse*

Schritt 1 – Zentrale Prozesse benennen

Nr.	*Was sind die zentralen Prozesse in Ihrem Unternehmen?*	*Läuft dies täglich ab?*	*Muss es IMMER laufen können?*
1			
2			
3			
4			

Beispiel:

1	Rohfischprodukte müssen immer **gekühlt** werden können.	*Ja*	*Ja*

Schritt 2 – Alternativen finden

Nr.	*Was ist eine mögliche Alternative, wenn der Prozess so nicht laufen kann?*

Beispiel:

1	Partnerunternehmen anfragen, ob diese Kapazitäten zum Kühlen haben. Zulieferer anfragen, ob Anlieferung verzögert werden kann.

Dokumentation offline bereitstellen

Tag 2 nach dem Angriff bei EiLand. Es fehlt nach wie vor der Zugriff auf Kundeninformationen, Verarbeitungsinformationen und Bestellungen, wodurch weder Waren erzeugt noch Kundenbestellungen abgehandelt werden können. Das Geschäft liegt nach wie vor still. Kunden sind verärgert über die Verzögerungen und Unsicherheiten.

Im Angriffsfall haben Sie womöglich keinen Zugriff auf Ihre Daten. Dazu gehören Kontaktdaten von externen Dienstleistern, der Kundschaft und Mitarbeitenden, genauso wie Auftragslisten oder Ähnliches.

Wir empfehlen Ihnen, jene Dokumente, die für den laufenden Betrieb unerlässlich sind (beispielsweise wichtige Telefonnummern), für den Notfall bereitzustellen. Diese sollten in Papierform ausgedruckt und an einem definierten und zugänglichen Platz abgelegt werden (beispielsweise in einem Notfallsordner oder Tresor). Zudem sollte sichergestellt werden, dass diese regelmäßig aktualisiert werden. Im Idealfall einigen Sie sich in Ihrem Unternehmen auf folgende Punkte: Wo werden die Dokumente abgelegt? Wie oft werden die Unterlagen neu ausgedruckt? Wer ist dafür zuständig?

Beispiele für relevante Unterlagen, die in Papierform vorliegen sollten:

- Notfallplan
- wichtige Telefonnummern (z.B. wichtigste Geschäftspartner, Kundschaft, Mitarbeitende, externe Dienstleister), evtl. eigene Listen für einzelne Abteilungen
- Grundlegende Informationen, damit der Betrieb im Angriffsfall weiterlaufen kann (z.B. was soll produziert werden. Was braucht man dafür?)
- Systemdokumentationen und Kennwörter (im Safe oder bei Versicherung).

Arbeitsblatt *Dokumentation* (1/2)

Wen müssen sie immer kontaktieren können (z.B. IT-Firma, Zulieferer, Kund*innen, ….)

Wen	*Wofür*

Beispiel:

Fischlieferanten	Änderung Anlieferungszeiten/-modalitäten

Arbeitsblatt *Dokumentation* (2/2)

Welche Informationen müssen immer verfügbar sein (z.B. Wochenplan, Notfallhandbuch, …)

Dokument	*Wo soll dieses abgelegt werden?*	*Wie oft soll es aktualisiert werden?*	*Wer macht das?*	*Allfällige Anmerkungen*

Beispiel:

Lieferantenliste mit Namen, Telefonnummern	Büro, Safe	Halbjährlich (1.12., 1.6.)	Frau Huber	Unbedingt auch Handynummern für Erreichbarkeit im Notfall!

Kommunikation planen

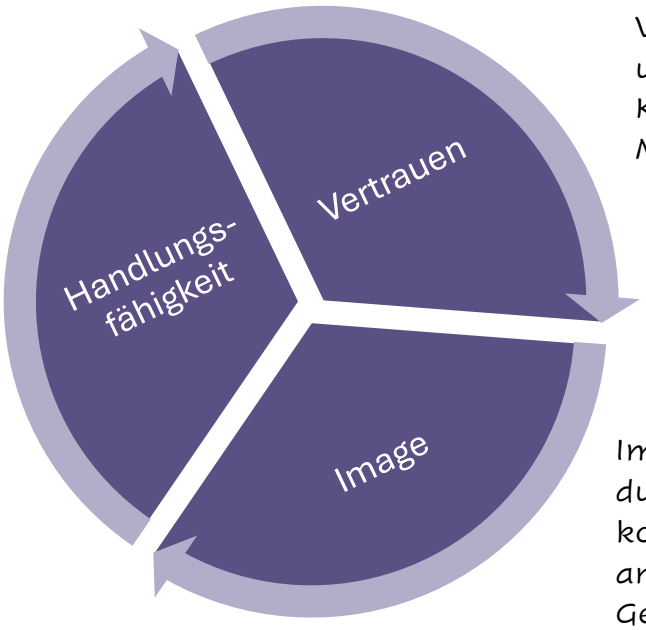
Wenn über Cybersecurity gesprochen wird, wird am öftesten auf das Thema „Kommunikation“ vergessen. Sie fragen sich warum das wichtig ist? Denken Sie sich in das nachfolgende Szenario hinein und entscheiden Sie für sich selbst, ob sie durchs Kommunikationslabyrinth irren oder doch lieber einen gut markierten Weg gehen wollen.

Der Cyberangriff auf EiLand hatte unter anderem auch Auswirkungen auf die Kommunikationskanäle der Firma: Nichts geht mehr! Silvia, die Vertriebsmitarbeiterin bei EiLand ist verzweifelt. Normalerweise erreicht sie die Kundschaft und Lieferanten per E-Mail und Telefon, um Bestellungen zu besprechen. Doch heute ist sie am Verzweifeln und etwas hilflos, da nicht klar ist, was sie tun kann. Einen Kunden kennt sie auch privat, weshalb dieser sie am privaten Smartphone kontaktiert. Aber eigentlich weiß Silvia nicht, welche Informationen sie dem Kunden überhaupt geben darf. Thomas versucht Ware aus dem Lager zu holen, da die Spedition bereits wartet, aber er weiß nicht, wie und vor allem auch nicht was er bereitstellen soll. Er kann Silvia nicht kontaktieren, da die Telefonverbindung nicht funktioniert und eigentlich weiß niemand so recht, was aktuell läuft.

„… alle handeln im Moment wie ‚kopflose Hühner“

Die interne Kommunikation ist chaotisch und alle handeln wie „kopflose Hühner“. Die Mitarbeitende laufen ständig zur IT-Abteilung, um neue Probleme zu melden bzw. nach dem aktuellen Status zu fragen. Um das Chaos zu stoppen, benötigt es eine rasche Krisen-Kommunikation! Silvia initiiert bei ihrem Chef eine Besprechung und gemeinsam mit der Geschäftsführung, dem Office und der Marketingabteilung wird eine Kommunikationsstrategie festgelegt.

WARUM ist eine transparente Kommunikation von Vorteil?



Vertrauen schaffen und bewahren bei Kundschaft und Mitarbeitenden

Der Kundschaft die Möglichkeit geben, selbst zeitnah Sicherheits-maßnahmen zu erhöhen

Image der Firma schützen, durch präventive und korrekte Kommunikation, anstatt aufkommender Gerüchte

- Die Situation soll für alle Mitarbeitenden klar sein, damit
  - Keine falschen/ungewollten Informationen nach außen geteilt werden
  - Anrufe bei der IT minimiert werden (z.B. mein PC geht nicht mehr)
- Die Situation soll für alle Kunden/Partner transparent sein, damit
  - Keine falschen/ungewollten Informationen aufkommen
  - Anrufe bei der (IT-)Hotline minimiert werden
  - Professionelles Verhalten wird gezeigt und Vertrauen durch proaktive Meldung bleibt erhalten
  - Kunden/Partner haben die Möglichkeit, eigene Maßnahmen gegen Angriffe zu setzen

Doch **Achtung!** Transparenz heißt nicht, mit allen Informationen zu laufenden Vorgängen nach außen zu gehen. Es reicht das notwendigste offen zu kommunizieren, um externe Stakeholder vor potenziellen Schäden zu bewahren bzw. diese nicht im Ungewissen zu lassen. Seien Sie jedoch vorsichtig mit Informationen hinsichtlich laufender Ermittlungen, technischen Vorgehensweisen oder eingesetzter Soft- und Hardware. Damit geben Sie Hackern womöglich zu tiefe Einblicke und bieten eine erneute Angriffsfläche. Stimmen Sie sich unbedingt mit der technischen Leitung ab, was nach außen kommuniziert werden darf.

WER soll kommunizieren?

Das hängt stark davon ab an WEN Sie kommunizieren müssen und WIE Sie im Moment in der Lage sind zu kommunizieren und schlussendlich auch davon, WANN und WAS sie kommunizieren sollten.

An WEN und in welcher Reihenfolge könnte kommuniziert werden?

1. ALLE Mitarbeitende
2. Externe Dienstleister, die Zugang zu internen IT-Anwendungen haben
3. Kundschaft / Partnerunternehmen (mit Abhängigkeiten zu laufenden IT-Anwendungen, Schnittstellen, Netzwerken etc.)
4. Versicherung
5. Polizei
6. Meldepflichtige Behörden/Organisationen (z.B. DSGVO-Verletzungen innerhalb 72h, NIS, Private Endkunden und Kunden-/ Partnerunternehmen, externe Dienstleister, etc.)
7. Medien/Presse

WIE sollte kommuniziert werden?

Das WIE hängt sehr stark davon ab, welche Kanäle überhaupt möglich sind, deshalb finden Sie hier nur einige Ansätze, die sie verfolgen können. Wichtig ist, dass Sie sich Gedanken über eine Kommunikationsstruktur ohne Internet oder internes Netzwerk überlegen. Ohne Netz gibt es womöglich keinen Zugang zu Telefonie, E-Mail oder Kontaktdaten.

Intern	- Firmenkommunikationskanäle (z.B. Teams, Webex, Skype, Zoom) - Durchsage über Lautsprecher - Intranet - SMS oder sonstige Messaging Apps (WhatsApp, Signal,etc.) - Persönlich durch die Büros gehen
	- E-Mail - Anruf
Extern	- Firmenhomepage
	- Über die Presse/Medien (TV, Nachrichtenportale, Zeitungen)

Arbeitsblatt *Kommunikationswege*

Welche Kommunikationswege inkl. technischer Voraussetzungen werden aktuell genutzt und welche Alternativen könnten sie stattdessen nutzen?

Kommunikationsweg	*Technische Voraussetzungen*	*Mögliche Alternativen*

Beispiel:

Telefonieren (intern)	Internet, MS Teams	Anruf über private Handys
Telefonieren (extern)	Internet, MS Teams	Anruf über private Handys

WER übernimmt die Kommunikation?

Spielen Sie alle Personen, die an der Behebung des Problems mithelfen, soweit es geht frei. Deshalb könnten etwa Personen aus der Personal- oder Marketingabteilung die Kommunikation übernehmen oder auch die Geschäftsleitung.

Für die Kommunikation mit Kunden/Partnern sollte die Ansprechperson für den jeweiligen Kunden/Partner gebrieft werden und dann entsprechend kontaktieren.

WER soll WAS und WANN an WEN kommunizieren?

Abhängig von Zeitpunkt, aktuellem Erkenntnisstand und Zielgruppe werden unterschiedliche Informationen verbreitet. Versuchen Sie im Arbeitsblatt „Kommunikationsplan“ den auf Ihr Unternehmen zugeschnittenen Weg zu finden.

WANN	**WAS**	**WER (von wem?)**	**An WEN**
So schnell als möglich	• Kurze Information das ein Hackerangriff passiert ist • Vorläufige Stillschweige-Vereinbarung	z.B. HR	ALLE Mitarbeitende
So schnell als möglich	• Welche Anwendungen/Prozesse betroffen sind (sofern man das schon weiß)	z.B. IT	ALLE Mitarbeitende
So schnell als möglich, sofern Kunden-anwendungen betroffen sind	• Kurze Information das ein Hackerangriff passiert ist • Welche Kunden-Anwendungen betroffen sind (sofern man das schon weiß) • Das an der Behebung gearbeitet wird und laufend über neueste Erkenntnisse informieren wird • Man kann auch seine Kunden/Partner um Stillschweigen bitten, bis Situation intern klar ist	z.B. zuständige Kundenbetreuende	Partner XY, Partner AB
So schnell als möglich, sofern Gefahren/Schäden für Kunden möglich sind (durch gehakte Schnittstellen/ Interfaces)	Zusätzlich zu Punkt davor auch noch: • Welche Kunden-Anwendungen potenziell in Gefahr sind und welche Gefahr besteht	z.B. zuständige Kundenbetreuende	Partner XY, Partner AB
Sobald die erste Aufregung vorbei ist und die Wiederherstellung und Forensik im Gange ist	Wiederherstellung der internen Kommunikation, damit Austausch zwischen Abteilungen und Mitarbeitende notfallsmäßig funktioniert.	z.B. HR, IT	ALLE Mitarbeitende

Arbeitsblatt *Kommunikationsplan (1/3)*

Erstellen Sie ihre eigenen Vorlagen und Textteile, damit es im Notfall schneller geht und Sie nicht erst nach den richtigen Worten suchen müssen.

Beispiele:

Wann	*Was*	*Wer (von wem?)*	*An wen?*
So schnell als möglich	Liebe Kolleginnen und Kollegen, am dd.mm. um ca. hh:mm ereignete sich eine Cyber Attacke auf unsere IT-Infrastruktur. Im Moment können wir noch nicht abschätzen, was alles betroffen ist, wir halten Sie/euch jedoch auf dem Laufenden. Bis auf weiteres dürfen keine Informationen nach außen gegeben werden (weder an Kunden noch an Freunde oder Verwandte)! Wir bereiten eine offizielle Stellungnahme vor und werden euch diese so schnell als möglich für notwendige Informationsweitergaben zur Verfügung stellen. Vielen Dank! xxx	Personalabteilung	ALLE Mitarbeitenden
So schnell als möglich	Liebe Kundenbetreuende, um unsere Kunden proaktiv zu informieren und etwaigen Unsicherheiten und Gerüchten vorzubeugen, bitten wir euch um Weitergabe folgender Informationen von den jeweiligen Kundenverantwortlichen an unsere Kunden: <xxxx> Vielen Dank! xxx	Geschäftsführung	Kundenbetreuende
So schnell als möglich	Liebe Kolleginnen und Kollegen, um den Wiederherstellungsprozess der IT-Infrastruktur und den aktuellen polizeilichen Ermittlungen nicht zu gefährden, dürfen wir auf Anfrage von extern ausschließlich folgende Informationen weitergegeben werden: <xxxx> Vielen Dank! xxx	Geschäftsführung	Kundenbetreuende, Hotline- bzw. Office-Mitarbeitende

Kommunikationsplan (2/3)

Wann	*Was*	*Wer (von wem?)*	*An wen?*

Kommunikationsplan (3/3)

Wann	*Was*	*Wer (von wem?)*	*An wen?*

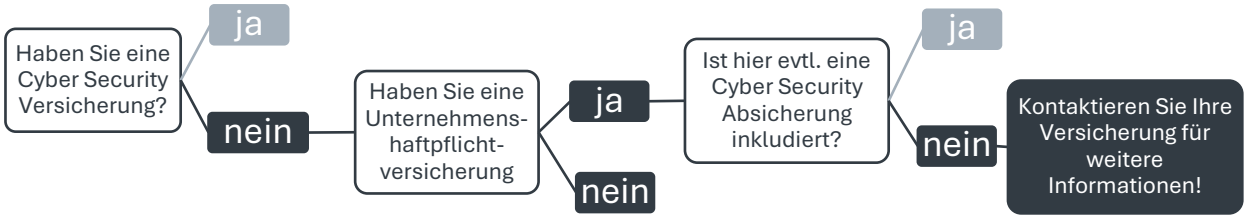
Versicherung

In der IT- und Cybersecurity-Branche ist es für Unternehmen enorm wichtig, über eine passende Versicherung nachzudenken. Es gibt mittlerweile eine Vielzahl an Versicherungsangeboten, die individuell auf die spezifischen Bedürfnisse eines Unternehmens zugeschnitten sind, abhängig von Faktoren wie Unternehmensgröße, Branche und der Art der zu schützenden Daten.

Ein kritischer Punkt bei diesen Versicherungen ist das korrekte Vorgehen im Falle eines Cyberangriffs. Es ist essentiell, dass solche Vorfälle sofort der Versicherung gemeldet werden, damit diese schnell reagieren und unterstützen kann. Wichtig dabei ist, dass Unternehmen nicht eigenständig agieren, sondern alle weiteren Schritte in enger Absprache mit ihrer Versicherung planen und durchführen. Dies kann von der ersten Schadensanalyse über rechtliche Schritte bis hin zu den Wiederherstellungsmaßnahmen der Systeme reichen.

Dieses koordinierte Vorgehen hilft nicht nur, den Vorfall effektiv zu bewältigen, sondern stellt auch sicher, dass die Richtlinien der Versicherung eingehalten werden und der Versicherungsschutz nicht gefährdet wird. Für Unternehmen im IT-Sektor ist es daher unerlässlich, sich genau mit den Details und Anforderungen ihrer Cyber-Versicherung vertraut zu machen und im Falle eines Cyberangriffs richtig zu handeln.

Quickcheck *Versicherung*



Verantwortlichkeiten klären

Mario interessiert sich nicht sonderlich für Cyber-Security-Themen, er fuchst sich eher bei Server-Admin Themen hinein. Aber zum Glück ist seine Kollegin Clara sehr bedacht auf das Thema. Sie ist zwar nicht explizit zuständig für die Umsetzung von technischen Maßnahmen, dafür gibt es einen externen Dienstleister. Dennoch kümmert sie sich um viele Themen in dem Bereich. Aus diesem Grund wurde sie nun von der Geschäftsführung als Hauptverantwortliche für das Thema auserwählt und bekommt auch die nötige Zeit, um den Notfallleitfaden aktuell zu halten und sich regelmäßig mit externen Dienstleistern auszutauschen, um für die neuesten Bedrohungen vorbereitet zu sein.

Wer hat sich in Ihrem Unternehmen das Thema „Cybersecurity“ auf die Fahnen geheftet?

Quickcheck *Verantwortlichkeit*

Welche Person in Ihrem Unternehmen fällt Ihnen spontan ein, wenn sie an die Begriffe unten denken?

Schreiben Sie pro Begriff spontan eine Person auf! (Mehrfach-Nennungen möglich)

Vertrauenswürdig _____

Gewissenhaft _____

IT bzw. EDV-affin _____

Sicherheit _____

Cybersicherheit _____

Es fällt immer wieder der gleiche Name? Perfekt! Sprechen Sie mit dieser Person und ernennen Sie sie zum/zur Cyber-Security Beauftragten:

_____

Notfallteam definieren

Mario weiß aus Erfahrung von anderen Firmen, dass man sich nicht auf Hotlines verlassen sollte und, dass so ein Angriff je nach Schwere und betroffenen Systemen viele Ressourcen binden kann (sowohl personell womöglich aber auch aus Hardware-Sicht). Da er in einer recht kleinen Firma arbeitet, hat sich die Firma über externe Dienstleister abgesichert, die im Notfall kontaktiert werden. Dadurch können Sie spontan Cybersecurity Experten und Expertinnen ins Boot holen, aber auch temporär benötigte Arbeitskräfte für die Wiederherstellungsphase. Die Basis dafür bildet jedenfalls ein internes Notfall-Team mit den unterschiedlichsten Mitarbeitenden.

Wissen Sie, wer im Notfall anpacken soll und kann?

Arbeitsblatt *Mögliches Notfallteam* (1/2)

Haben Sie ein Notfall-Team, das im Ernstfall weiß, was zu tun ist und vor allem wer was zu tun hat? Schreiben Sie hier möglichen auf, die im Ernstfall eingebunden werden können. Besetzen Sie jede Position mit einer möglichen Vertretung. Ziehen Sie diese Liste im Ernstfall heran, um die Aufgaben entsprechend zu verteilen.

Verantwortungsgebiet	*Personen*	*Telefon (Firma, Privat)*
NOTFALL **ERSTKONTAKT** bzw. **Leitung des Krisenstabs** *– ruft das Krisen-Team zusammen und leitet die ersten Schritte ein* *– ist primäre Ansprechperson für alle Fragen* *– (optional) leitet die regelmäßigen Krisen-Team Sitzungen oder benennt eine Person dafür*	Hauptverantwortlich (H):	
	Vertretung (V):	
Rechtliche Themen (z.B. Anzeige bei Polizei, DSGO, NIS, etc.):	H:	
	V:	
Forensik:	H:	
	V:	
Wiederherstellung:	H:	
	V:	
Interne Kommunikation (an Mitarbeitende)	H:	
	V:	
Externe Kommunikation (an Kunden und Presse	H:	
	V:	
Sonstiges	H:	
	V:	

Arbeitsblatt *Mögliche externe Dienstleister* (2/2)

Haben Sie Kontakte zu externen Dienstleistern, die Ihnen im Fall eines Angriffs helfen können? Schreiben Sie hier Ihre Partner-Firmen auf, mit denen Sie bereits in Kontakt sind und die Ihnen im Notfall helfen können:

Verantwortungsgebiet	*Firma*	*Kontaktperson (wenn vorhanden), Telefonnummer*
Forensik (um herauszufinden was überhaupt passiert ist)		
Wiederherstellung:		
Arbeitskräfte (zur Hilfe bei der Wiederherstellung)		
Hardware (Notebooks, Internet-Cube, Server, etc.)		
Versicherung		
Sonstiges		

Vorgehensplan vorbereiten –

im Notfall an aktuelle Gegebenheiten anpassen

Nachdem Mario über den Erst-Kontakt das Notfall-Team aktiviert hat, ist das externe Forensik-Team gerade dabei herauszufinden was passiert ist. Johannes (53) der Geschäftsführer von EiLand wurde schon vor 30min telefonisch informiert und ist gerade auf dem Weg zum Firmengelände. Auch wenn der Schock tief sitzt, während IT-Mitarbeitende den Angriff stoppen, ruft Johannes aus dem Auto heraus gerade alle für den Notfall vorgesehenen Personen für eine erste Krisenbesprechung zusammen.

Sie haben bereits wichtige Maßnahmen gelernt, damit Sie für den Ernstfall besser vorbereitet sind. Dennoch gibt es für den Ernstfall kein Koch-Rezept und Sie müssen ihre Aktivitäten der aktuellen Situation anpassen. D.h. in diesem Teil erstellen Sie einen Leitfaden mit Fragen und Aufgaben, die auf Ihr Unternehmen abgestimmt sind, um am Tag X strukturiert vorgehen zu können. Es macht Sinn diesen Leitfaden z.B. mit Ihrem aktuellen IT Dienstleister durchzugehen, oder wie bereits erwähnt mit einen potentiellen IT Dienstleister durchzugehen.

Im folgenden Abschnitt finden Sie Ideen zu Fragen und Aufgaben. Überlegen Sie welche Fragen könnten für die Analyse der Situation, den ersten Schritten und der weiteren iterierenden Vorgehensweise helfen.

Schritt 1 – Analyse

- Was ist betroffen?
    a) Welches System?

       _____

    b) Welche Assets?

       _____

    c) Netzwerk? Hardware?

       _____

    d) Welche Firmenstandorte?

       _____
- Was ist passiert? (Evtl. hier bereits externe Forensik hinzuziehen)
- Woher kam der Angriff? (Parallel zu allen weiteren Schritten)

Schritt 2 – Angriff stoppen, Ausbreitung verhindern

Überlegen Sie gemeinsam mit Ihren internen und externen Expert*innen, wie sie eine weitere Ausbreitung verhindern können. **Folgende Punkte dienen nur als Idee:**

- Clients und Server isolieren z.B. vom Netz trennen (Kabel abstecken, WLAN ausschalten), Server herunterfahren
- Nicht mit privilegierten Benutzerkonten (Administratorkonten) bei einem potenziell infizierten System anmelden, während es sich in einem internen Produktionsnetzwerk befindet oder mit dem Internet verbunden ist!
- Verifizierung aller Konten (vor allem Administratoren).
    - Sind alle Administratorkonten legitim angelegt oder gibt es Konten, die keinem Mitarbeitenden zugeordnet werden können?

    - Gibt es Standardbenutzerkonten, die nicht nur Benutzerrechte, sondern auch Administratorrechte haben? Die Malware könnte diese Konten ändern und verwenden.
- Gibt es DNS-Auflösungsversuche auf Clients oder fehlgeschlagenen DNS-Auflösungsversuchen (NXDOMAIN) auf DNS-Server? Diese könnten auf Schadsoftware hinweisen. Prüfen Sie die lokale Windows-Firewall der betroffenen Systeme (z. B. auf neue RDP-Freigaben).
- Blockieren Sie vorerst nicht unbedingt erforderliche Remoteverbindungen (RDP, SSH, Terminal-Server, Teamviewer, etc.)
- Monitoring aufrechterhalten bzw. wieder aktivieren!
  Überwachen Sie den Netzwerkverkehr und führen Sie Antivirenscans durch, um weitere Infektionen und böswillige Zugriffe zu erkennen bzw. zu verhindern. Dies umfasst u. a. Webbrowser, E-Mail-Clients, RDP/VNC-Verbindungen, Benutzer-Logins, Passwörter für Fachverfahren sowie andere Anwendungen wie PuTTY, FileZilla, WinSCP, etc.
- Mitarbeitende informieren und zur Vorsicht aufrufen!
- Bevor sie ihre Backups wieder einspielen, lassen sie diese ggf. von externen Forensikern prüfen, ob diese sauber und somit nicht kompromittiert sind.
- Erarbeiten Sie mit Cybersecurity-Profis, weitere Maßnahmen, die für Ihr Unternehmen sinnvoll sind, um eine Ausbreitung zu verhindern.

- _____
- _____
- _____

Schritt 3 – Krisenstab bilden

Bilden Sie anhand der vorhandenen Notfallkontakte einen Krisenstab! Wer vom vorgesehenen Notfallteam ist aktuell verfügbar und in den nächsten Stunden/Tagen für folgende Themen zuständig?

Koordination regelmäßiger Abstimmungstermine:	
Leitung der Termine:	
Leitung Forensik:	
Leitung Wiederherstellung/Technische Maßnahmen:	
Leitung Kommunikation	Intern: Kunden: Presse: *(ergänzen Sie die Liste oder streichen Sie Themen, die für ihr Unternehmen nicht relevant sind)*
Leitung Rechtliche Themen	Anzeige Polizei: DSGVO: NIS-Meldung: *(ergänzen Sie die Liste oder streichen Sie Themen, die für ihr Unternehmen nicht relevant sind)*
Sonstige relevante Themen	

Schritt 4 –Wiederherstellung

Die Situation während bzw. nach einem Angriff ist immer eine Momentaufnahme und kann sich gerade am Anfang rasch verändern. Deshalb ist es wichtig, sich im Krisenstab in regelmäßigen Abständen auszutauschen. Am Anfang in kürzeren Abständen (im Stundenbereich) und später in immer längeren Abständen. In den Terminen teilen alle Beteiligten Ihre Erkenntnisse oder Fragen und dementsprechend werden Aufgaben verteilt und die Vorgehensweise ständig angepasst. Schreiben Sie die Aufgabenverteilung für die aktuelle Phase auf und prüfen Sie den Fortschritt im nächsten Termin. Diese Iteration läuft solange bis die IT-Infrastruktur wiederhergestellt ist.

Sie fühlen sich überfordert? Nur allzu verständlich in dieser komplexen Situation. Scheuen Sie nicht externe Professionisten hinzuzuziehen! Diese können Sie vor allem in der akuten Phase unterstützen, damit Sie die richtigen Entscheidungen treffen.

Rechtliche Maßnahmen

Nachdem der Angriff auf EiLand bei der Polizei gemeldet wurde, ist diese aktuell am Firmengelände und befragt gerade Mario, zu persönlichen Beweggründen für eine mögliche Täterschaft. Mario ist in erstem Moment etwas überfordert mit der Situation und will eigentlich nur helfen, dass Unternehmen wieder auf Schiene zu bringen. Stattdessen befindet er sich in einer Polizeibefragung und fühlt sich sichtlich unwohl.

Polizei

Eine Anzeige bei der Polizei ist nicht verpflichtend, aber definitiv ratsam für die weitere Abwicklung z.B. bei der Versicherung, Behörden oder mit ihren Vertragspartnern.

Für weitere Informationen und Hilfe oder bei einem Verdacht auf Internetkriminalität, wenden Sie sich bitte an:

- das Bundeskriminalamt - Meldestelle für Internetkriminalität: against-cybercrime@bmi.gv.at

ODER wenn Sie durch eine Straftat geschädigt wurden, können Sie die Straftat anzeigen:

- in jeder Polizeidienststelle

Beachten Sie, dass mögliche Beweise gerichtsfest erhoben und alle Vorgänge entsprechend dokumentiert werden müssen.

Lösegeld

Lösegeld-Zahlungen sind nur der allerletzte Ausweg, denn…

1. Sie haben keine Garantie, dass verschlüsselte Dateien entschlüsselt werden, oder abgezogene Daten gelöscht.
2. Sie wissen nicht an wen Sie das Lösegeld zahlen. Womöglich unterstützen Sie damit eine terroristische Organisation und machen sich selbst straftätig.
3. die Organisation der Übergabe (meist wird virtuelle Währung gefordert) sowie die Beschaffung des Geldes kann mehrere Tage dauern und sind somit auch keine schnelle Lösung.

NIS

Sofern Ihr Unternehmen in die Sicherheit der Netz- und Informationssysteme (NIS)-Richtlinie bzw. NIS2-Richtlinie fällt, ist eine Meldung des Sicherheitsvorfalls auf der NIS-Meldeplattform nötig.

DSGVO/Datenschutz

Sind sensible/persönliche Daten abgezogen worden oder besteht die Möglichkeit?
Ziehen Sie einen DSGVO-Experten hinzu, um sicher zu gehen bei Bedarf Ihren rechtlichen Meldepflichten (meist innerhalb von 72h) nachzukommen.

Nach dem Angriff – Aufarbeitung des Vorfalls

Nach insgesamt 7 Wochen, sind die letzten Aufräumarbeiten nach der Cyberattacke auf EiLand abgeschlossen und die Systeme und fast alle Daten wieder hergestellt und abgesichert. Leider nicht ganz ohne Datenverluste, aber diese sind zum Glück klein. Die Forensik hat letzte Woche die Ergebnisse geschickt, weshalb Johannes nun zu einem abschließenden Lessons Learned einlädt. Er möchte den Vorfall mit allen Beteiligten aufarbeiten und die IT-Infrastruktur sowie den internen Notfallplan verbessern, denn er weiß, nach dem Angriff ist potenziell vor dem (nächsten) Angriff.

Und wenn er eines gelernt hat, dann folgendes:

Also vor etwas, was du nicht weißt, kannst du dich nicht schützen

Berufen Sie abschließend einen Workshop ein, um das Geschehene zu aufzuarbeiten. Lernen Sie aus Ihren Erfahrungen und verbessern Sie Ihre organisatorischen und technischen Abläufe. Es muss keine Cyberattacke sein, die Sie das nächste Mal erwischt, es reicht schon ein abgerissenes Netzwerkkabel im Zuge von Bauarbeiten, die einen kurzfristigen Ausfall erzeugen könnten.

Ideen für einen Workshop mit dem Kern-Team:

- „Lessons Learned“-Workshop
- Retrospektive (siehe Anhang *Retrospektive zur Vorfallsaufarbeitung*)
- Büropflanzen-Frage:
  „Mal angenommen unsere Büropflanze könnte sprechen, wie hätte sie die Situation erlebt? Was würde sie nun ansprechen, was wir jetzt noch nicht angesprochen haben?“

Sie können auch Feedback von allen Mitarbeitenden einholen, um ein Stimmungsbild nach dem Angriff einzufangen. Dazu gibt es folgende Möglichkeiten

- Happiness Door Methode (wobei anstatt Haftnotizen an der Tür, evtl. ein Online Board nutzen, oder eine Pinnwand/Wand in einem öffentlichen Bereich)
- Fragenbogen (online oder ausgedruckt)
- Aufruf an alle freie Rückmeldungen zu geben (per Mail oder persönliches Gespräch)

Abschlussbemerkungen

Die vorangegangene Erhebung und Auswertung, sowie die Umsetzung als Leitfaden und Workshop wurden von DIH Süd gefördert.

Dieser Leitfaden ist auf Basis der Erfahrungen, erhoben durch Interviews mit Experten und Expertinnen sowie betroffenen Unternehmen (Opfern von Cyberangriffen), entstanden. In Vorbereitung auf diese Interviews und in weiterer Folge zur Aufbereitung einzelner Inhalte wurden folgenden Quellen herangezogen:

- BKA (Jänner 2023): Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit 2021. Fortschrittsbericht 1/2023. Hg. v. Bundeskanzleramt (Österreich).
- BSI: Ich habe einen Vorfall – Checkliste Technik. Online verfügbar unter https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik.html, zuletzt geprüft am 03.07.2024.
- BSI: IT-Notfallkarte - Ihr Einstieg ins Notfallmanagement. Online verfügbar unter https://www.bsi.bund.de/dok/13003500, zuletzt geprüft am 03.08.2023.
- BSI (2014): Leitfaden Krisenkommunikation Krisenkommunikation. Hg. v. Bundesministerium des Innern (Deutschland). Berlin.
- BSI (2022): Erste Hilfe bei einem schweren IT-Sicherheitsvorfall. Hg. v. Deutsches Bundesamt für Sicherheit in der Informationstechnik. Bonn.
- Bundeskriminalamt; Charter of Trust; Deutscher Industrie- und Handelskammertag e.V.; eco – Verband der Internetwirtschaft e.V.;, Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V.; VOICE - - Bundesverband der IT-Anwender e.V.; Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (2019): TOP 12 Maßnahmen bei Cyber-Angriffen, zuletzt aktualisiert am 03.08.2023.
- Polizei (2015): IT-Sicherheit: 7 Tipps für Unternehmen und öffentliche Einrichtungen. Hg. v. Österreich (Polizei).
- WKO: Ich habe einen Vorfall – Checkliste. Online verfügbar unter https://www.wko.at/service/innovation-technologie-digitalisierung/ich-habe-einen-vorfall-checkliste.html, zuletzt geprüft am 03.08.2023.
- WKO (2018): it-safe.at – das IT-Sicherheitsprojekt für KMU. Hg. v. Wirtschaftskammer Österreich - Bundessparte Information und Consulting. Wien.

DIHSÜD Digital Innovation Hub

CAMPUS 02 FACHHOCHSCHULE DER WIRTSCHAFT

Der DIH SÜD wird unterstützt von:

FFG Forschung wirkt

Das Land Steiermark

LAND KÄRNTEN

Anhang - *Retrospektive zur Vorfallsaufarbeitung*

Die Retrospektive, eine Methode aus der agilen Softwareentwicklung nach Scrum, könnte ein guter Einstieg in Ihren Aufarbeitungsworkshop sein. Dazu benötigen Sie einen Besprechungsraum und…

- Whiteboard oder Flipchart
- Stifte
- Haftnotiz-Zettel

oder

- Laptop/Smartphone pro Teilnehmer*in
- Beamer
- Retro Online Tool
  (z.B. Easy Retro, Miro, retro.io, Jira Add-Ins,)

1. **Intro**
   - Danksagung
     Danke an alle Beteiligten aussprechen, dass sie während des Angriffs und der Wiederherstellung vermutlich lange Arbeitstage hatten

   - Ziel des Workshops
     - funktionierende Abläufe aufzeigen, beibehalten und dokumentieren,
     - lückenhafte oder fehlende Abläufe identifizieren, geeignete Abfolgen erstellen und dokumentieren à ggf. im Zuge einer Notfall Übung auch testen

   - Status Quo (sofern vorhanden)
     Art des Angriffs und Einfallstor nochmal kurz für alle darlegen und dann klären, ob die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-)Prozessen durch relevante Maßnahmen adressiert und behoben wurden?
     (Hinweis: dieser Teil kann auch schon vorab mit der IT abgestimmt werden, um das Ergebnis allen zu präsentieren)
     - Aufzeigen was bereits umgesetzt wurde
     - Aufschreiben was noch umgesetzt werden soll (gleich auf Notizzettel oder Liste schreiben und für später bereithalten)

2. **Retrospektive**
   - Retro erklären
     - Zweck: ein Format zur Reflexion und Verbesserung der Zusammenarbeit
     - Ablauf: es werden drei Fragen gestellt bzw. es gibt drei Kategorien, zu denen alle Teilnehmenden etwas schreiben können:
       - KEEP (because GOOD): Was ist gut gelaufen?
       - STOP (because BAD): Was ist schlecht gelaufen?
       - START: Was können wir in Zukunft versuchen?
   - Feedback sammeln
     - Alle Teilnehmenden schreiben gleichzeitig auf und hängen ihre Zettel oder posten sie zur entsprechenden Kategorie
     - Es können andere Beiträge durchgelesen und unterstützt werden durch ein „Like“ oder einen Notizzettel dranhängen
   - Feedback laut vorlesen
     - Bei gleichen oder ähnlichen Themen à Gruppieren
     - Bei Unklarheiten nachfragen, klären und aufschreiben

        - Gerne auch zusätzliches Feedback mitaufnehmen

- Feedback kategorisieren
    - Gibt es beim positiven Feedback trotzdem etwas zu tun? z.B. gut gelaufene Abläufe zu dokumentieren, dann am besten gleich mit Prio niedrig bewerten, die restlichen Themen können vorerst ignoriert werden
    - Betrifft ein Thema mehrere/übergreifende Fachbereiche oder nur einen Fachbereich? Markieren sie die Themen z.B. mit A (alle) und F (Fachbereich)

3. PAUSE (15-20min)

4. Ableitung gruppenübergreifender Maßnahmen

Zuerst werden alle Themen aufgegriffen, die alle betreffen. Sind es sehr viele, dann sollten diese zuerst noch priorisiert werden, je nachdem von welchem das größte Risiko ausgeht, einen Schaden für das Unternehmen zu verursachen.

Die Maßnahmen sollten am Ende niedergeschrieben, priorisiert und an eine Person verteilt werden.

5. Ableitung Fachbereichs-spezifischer Maßnahmen

Selbes Vorgehen wie bei Punkt 5, jedoch nur innerhalb des betroffenen Fachbereichs. Je nach Umfang kann dieser Teil auch an einem anderen Tag durchgeführt werden.

6. Gemeinsamer Abschluss

Am Ende kommen noch einmal alle zusammen und es werden noch die Maßnahmen aus den Fachbereich-Teams vorgestellt, sofern es hier welche gab.

Danach wird beschlossen, bis wann die neuen Maßnahmen umzusetzen sind und der Notfallplan entsprechend anzupassen ist. Zusätzlich wird ein gemeinsamer Termin für ein Review der Umsetzungen festgelegt.