AUSWIRKUNGEN AUF DIE SICHERHEIT FÜR DEN INDUSTRIESEKTOR WÄHREND UND NACH COVID-19

FEDIL
The Voice of Luxembourg's Industry

INHALTSVERZEICHNIS

VORWORT

FEDIL, The Voice of the Luxembourg's Industry, rief in Zusammenarbeit mit dem **Wirtschaftsministerium** (Abteilung für E-Commerce und Informationssicherheit) ein **Forum zur Cybersicherheit** ins Leben, das der verarbeitenden Industrie (IND) gewidmet ist. Dieses Forum folgt den Prinzipien eines **« Information Sharing and Analysis Center »** (ISAC).
Die Aufgabe des IND-ISAC besteht darin, die Zusammenarbeit im Bereich der Cybersicherheit innerhalb des Sektors der Fertigungsindustrie in Luxemburg und der Großregion zugunsten der Attraktivität des Ökosystems zu fördern.

Wie es in den politischen Richtlinien für die Europäische Kommission 2019-2024 heißt, « *we need to move from "need to know" to "need to share"* ». Der Auftrag wird erreicht durch (1) Informations- und Wissensaustausch zwischen vertrauenswürdigen Vertretern der Mitgliedsorganisationen und (2) die Verbreitung von Risikoinformationen der verarbeitenden Industrie, die für die Öffentlichkeit relevant sind.

Das IND-ISAC strebt die Schaffung einer gemeinsamen Sprache / Taxonomie an, um Synergien zu fördern und ein gemeinsames Verständnis der Risiken innerhalb des Unternehmens, der Gruppe und des Ökosystems zu teilen, indem es folgendes hervorhebt:

- die Wichtigkeit einer informierten Governance, d.h. einer Cybersicherheitsgovernance auf Sektor-, Gruppen- oder Unternehmensebene, auf der Grundlage möglichst vieler Sachinformationen (Vorteile für CISO's), und
- die Wichtigkeit des Risikomanagements und vor allem die Verwendung von möglichst vielen objektiven und sachlichen Informationen, und
- wie wichtig es ist, die Kommunikation zwischen technischer und organisatorischer Sicherheit unter Einbeziehung des Top-Managements zu implementieren.

Das IND-ISAC setzt sich aus Cybersicherheitsvertretern von Unternehmen aus verschiedenen Branchen zusammen.

Das folgende Dokument ist das erste Ergebnis des IND-ISAC und konzentriert sich auf die COVID-19-Krise.

Das IND-ISAC wird seine Arbeit fortsetzen, indem es Unternehmen in die Lage versetzt, Informationen, Erfahrungen, Wissen und bewährte Praktiken in einem Klima des Vertrauens unter Gleichgesinnten auszutauschen. Es zielt darauf ab, sektorspezifische Risikoszenarien, Schwachstellen und Bedrohungen zu identifizieren und bietet Unternehmen eine konkrete Anleitung zur Durchführung einer Risikomanagement-Analyse.

Wenn Sie dem IND-ISAC beitreten und ein aktives Mitglied werden möchten, laden wir Sie herzlich ein, sich mit unserem Team in Verbindung zu setzen.

FEDIL

EINFÜHRUNG

Wie viele andere Sektoren wurden auch die Industrie und das verarbeitende Gewerbe von der sanitären und wirtschaftlichen Krise, die durch die COVID-19-Pandemie ausgelöst wurde, hart getroffen. Die Krise ermöglichte es ihr jedoch auch, die Schwachstellen von Betriebskontinuitätsplänen und von Krisenmanagement aufzudecken und stellte somit einen realen Testfall für das Risikomanagement dar. Es ist daher wichtig, aus den gewonnenen Erkenntnissen zu lernen, um die Leistung in nachfolgenden Krisen (oder nachfolgenden Wellen der aktuellen Krise) zu verbessern.

Kurz nach Ausbruch der Krise gingen die meisten Organisationen von einem normalen in einen Ausnahmezustand über, in dem die Produktivität entweder stark reduziert oder vorübergehend eingestellt wurde. Die unerwartete Situation wurde von unvorhergesehenen Problemen begleitet, die schnelle und unkonventionelle Lösungen erforderten. Einige Organisationen schafften es, diesen Zustand innerhalb von Tagen zu verlassen, andere benötigten Wochen – doch dann setzte sich ein “neuer normaler” Zustand durch.

Im “neuen Normalzustand” ist die Sicherheit oft geschwächt, weil Entscheidungen in Eile getroffen wurden oder weil frühere Bedingungen (wie ein sicheres Umfeld) nicht mehr gegeben waren. Die COVID-19-Krise sollte jedoch als eine einzigartige Gelegenheit gesehen werden, neue Sicherheitskonzepte (insbesondere im Zusammenhang mit Home Office) einzuführen und sie unter realen Bedingungen zu testen nicht nur für die Dauer der Krise, sondern auch nach der Rückkehr ins Büro.

Für den Industriesektor sind die Kerngeschäftsschritte Material, Warenproduktion und Verkauf, weshalb die wichtigsten Sicherheitsaspekte mit Produktionskürzungen und Umsatzeinbußen verbunden sind. Es hat sich in der Krise gezeigt, dass sie entweder direkt (z.B. durch staatliche Maßnahmen wie die Schließung von Grenzen) oder indirekt durch Abhängigkeiten – seien es Kunden oder Investoren – beeinflusst werden können.

INHALT DIESES DOKUMENTS

Dieses Dokument befasst sich mit den Veränderungen in der Risikolandschaft, die während der COVID-19-Krise festgestellt oder durch sie verursacht wurden. Es behandelt insbesondere die folgenden Themen:

- wichtige Risiken, die vor der Krise vernachlässigt wurden;
- neue Risiken, die während der Krise aufgetreten sind;
- Überlegungen zur Überprüfung der Bewertung der Risiken (Änderung der Wahrscheinlichkeit und/oder der Auswirkungen bestehender Risikoszenarien);
- Schwachstellen, die beim Übergang zur “neuen Normalität” entstehen;
- Sicherheitserwägungen für die Rückkehr zur Normalität;
- Möglichkeiten zur langfristigen Verbesserung der Sicherheit.

NEUE ERKENNTNISSE AUS UND FÜR DIE BRANCHE

1/UNTERER TEIL DER LIEFERKETTE

SCHLÜSSELERKENNTNISSE

Die Lieferkette gehört zu den wichtigsten Aktivposten der verarbeitenden Industrie, da sie sich direkt auf die Produktion und damit auf das Kerngeschäft auswirkt. Daher wurden die Risiken im Zusammenhang mit der Beschaffung von Lieferungen bereits vor der Krise weitgehend bewertet. Tatsächlich waren zum Zeitpunkt der Krise ausreichende Lagerbestände und Ersatzlieferanten verfügbar.

Bislang wurden die Risiken im Zusammenhang mit dem hinteren Teil der Lieferkette nur wenig beachtet. Die Krise traf jedoch nicht nur die Lieferanten, sondern auch die Kunden, was zu einem starken Rückgang der Nachfrage nach den produzierten Gütern führte. In kurzer Zeit füllten sich die Lager und die Produktion musste gedrosselt oder sogar gestoppt werden – auch wenn die Krise zu Beginn keine direkten Auswirkungen auf den Hersteller hatte. Die Notwendigkeit, die Produktion zu drosseln, führte zu hohen Fixkosten gegenüber dem vergleichsweise niedrigen Einkommen und bedrohte die Existenz des Unternehmens.

SCHLÜSSELRATSCHLÄGE

A. NEUE KRISENSPEZIFISCHE RISIKEN ERKENNEN

- Risiko des Produktionsstillstand aufgrund mangelnder Nachfrage einbeziehen, unter Berücksichtigung aller Abhängigkeiten des hinteren Teils der Lieferkette.

2/LOKALE VS GLOBALE EINSCHRÄNKUNGEN

SCHLÜSSELERKENNTNISSE

Als die Pandemie Europa und die ganze Welt traf, war sie im Fernen Osten bereits seit etwa zwei Monaten bekannt. Infolgedessen setzte auch in diesen Regionen die Erholungsphase früher ein, so dass Konkurrenten Vorteile gegenüber noch eingeschränkten Unternehmen erlangen konnten.
Ähnliche Beobachtungen konnten auch in einem kleineren Kreis beobachtet werden. Die europäischen Regierungen haben die Beschränkungen und deren Aufhebung nicht koordiniert, wodurch selbst innerhalb Europas Marktungleichheiten entstanden.
Ein Problem, das sehr spezfische auf kleine Länder wie Luxemburg zutrifft, sind die Steuergesetze für Pendler, die eine Menge von Telearbeitstagen darstellen pro Jahr, das von Land zu Land unterschiedlich ist.

SCHLÜSSELRATSCHLÄGE

A. NEUE KRISENSPEZIFISCHE RISIKEN ERKENNEN

- Risikos des Verlusts von Kunden aufgrund staatlicher Beschränkungen einbeziehen, die nur lokal oder länderübergreifend nicht abgesprochen sind.

SCHLÜSSELERKENNTNISSE

Im Allgemeinen dauerte die Wiederaufnahme der Aktivitäten sehr lange (bis zu mehreren Wochen), obwohl Pläne zur Wiederherstellung nach Katastrophen existierten. Dies war auf mehrere Faktoren zurückzuführen.
Aufgrund der sanitären Einschränkungen wurden die meisten Mitarbeiter nach Hause geschickt, um von zu Hause aus zu arbeiten. Infolgedessen war das Schlüsselpersonal, das in den Notfallplänen für die Wiederaufnahme der Aktivitäten vorgesehen war, vor Ort nicht verfügbar. Die physische Anwesenheit war jedoch oft erforderlich, weil entweder der Zugang von der Ferne aus Sicherheitsgründen nicht gestattet war oder weil Prozesse nicht digitalisiert wurden (was im industriellen Sektor häufig der Fall ist).
Darüber hinaus wurde die Ausgangssperre nicht mit einem Mal aufgehoben, sondern es galten Einschränkungen (wie körperlicher Abstand, Tragen von Masken, Personalabbau ...), so dass die Unternehmen nicht einfach ihre gesamte Belegschaft reaktivieren konnten. Es stellte sich jedoch heraus, dass es oft nicht klar war, welches Personal zuerst reaktiviert werden sollte.
In Luxemburg sind mehr als 50% des Personals im Gesundheitssektor Pendler. Da die Regierung die Schließung der Grenzen als eines der größten Risiken für diesen Sektor betrachtet, wurde vorgeschlagen, das Gesundheitspersonal in Luxemburg in Hotels unterzubringen. Auch wenn der Anteil der Pendler im Industriesektor nicht so hoch ist, besteht das gleiche Problem.

SCHLÜSSELRATSCHLÄGE

A. BEKANNTE RISIKEN NEU BEWERTEN

- Regierungen könnten bei der korrekten Einschätzung des Risikos im Zusammenhang mit Pandemien versagen. Wenn es zu einem potenziellen Krisenausbruch kommt, sollten Sie eine eigene Risikoeinschätzung und Informationsbeschaffung durchführen, um vor dem Ausbruch einer Krise bereit zu sein.

B. BESTEHENDE SICHERHEITSMAßNAHMEN VERBESSERN

- Entwerfen Sie Geschäftskontinuitätspläne die es erlauben, Geschäftsprozesse aus der Ferne zu verwalten.
- Entwerfen Sie den Notfallwiederherstellungsplan so, dass er aus der Ferne ausgeführt werden kann.
- Definieren Sie Prioritäten, die es ermöglichen, die Reihenfolge festzulegen, in der das Personal reaktiviert wird.
- Berücksichtigen Sie die Krisenmanagement-Fähigkeiten der Regierungen sowie die Bereitschaft der Bevölkerung, den Anweisungen der Regierung zu folgen.
- Überprüfen Sie, ob Ihr Krisenmanagementverfahren auch lang anhaltende Krisen behandeln.
- Verbessern Sie Ihre Möglichkeiten, Signale einer sich anbahnenden Krise frühzeitig zu erkennen.

C. ZUSÄTZLICHE MAßNAHMEN ERWÄGEN

- Lebensraum für Schlüsselpersonal schaffen, wenn Grenzen geschlossen sind oder Gefahr laufen, geschlossen zu werden.
- Implementierung digitaler Werkzeuge und Lösungen, die repetitive Arbeiten digitalisieren können.

4/AUSSETZUNG DER INTERNEN INFRASTRUKTUR NACH AUSSEN

Mitarbeiter, die von zu Hause aus arbeiteten, mussten auf die Informations- oder Steuerungssystemezugreifen, die oft nur innerhalb des Unternehmensnetzwerks und nicht in der Cloud verfügbar waren. Während eine solche Vorgehensweise unter normalen Umständen von der Vertraulichkeit her sicherer ist, konnten die Mitarbeiter während der Krise zunächst nicht von zu Hause aus arbeiten.

Als Notmaßnahme machten einige Unternehmen kritische Dienste (einschließlich industrieller Kontrollsysteme) vom Internet aus verfügbar, da die Unternehmen die Verfügbarkeit für wichtiger als die Integrität hielten (oder weil sie sich der Auswirkungen auf die Sicherheit nicht bewusst waren). In der Industrie sind solche Systeme jedoch oft proprietär, veraltet oder Relikte von Übernahmen und daher oft von Natur aus unsicher (mit Schwachstellen, schlechten Sicherheitsstandards, Standardpasswörtern, ...). Infolgedessen sind viele kritische Systeme heute selbst nicht zielgerichteten Angriffen ausgesetzt, wodurch eine riesige Sicherheitslücke entsteht.

Eine weitere Möglichkeit wäre der Aufbau von virtuellen privatenNetzwerken (VPN). VPN-Lösungen waren jedoch oft nicht vorhanden, und wenn sie vorhanden waren, waren die persönlichen Geräte nicht für die Verbindung mit ihnen konfiguriert. In der Tat muss nicht nur ein Software-Client installiert und eingerichtet werden, sondern es müssen auch starke Authentifizierungs-Token (bei denen es sich häufig um physische Geräte handelt) verteilt werden.

Darüber hinaus hat die Möglichkei, dass Mitarbeiter sich mit ihren eigenen Geräten an das interne Netzwerk anzuschließen, enorme Auswirkungen auf die Sicherheit. Da das Unternehmen keine Kontrolle über diese Geräte, beziehungsweise über deren Sicherheit hat, sind die meisten dieser Geräte nicht angemessen vor Malware und Hackerangriffen geschützt. Hinzu kommt, dass den Mitarbeitern oft nicht bewusst ist, welchen Bedrohungen sie ausgesetzt sind.

Die Krise machte auch Mängel in der Gestaltung einiger sicherheitsrelevanter Arbeitsabläufe deutlich. Wenn das Ablaufintervall für Passwörter zu kurz eingestellt war, liefen die Passwörter ab, wenn das Personal aus der Ferne arbeitete. Dies führte zu einem Teufelskreis, bei dem sich die Mitarbeiter mit der Infrastruktur des Unternehmens verbinden mussten, um ihr Passwort zu ändern oder zurückzusetzen, was ihnen jedoch nicht möglich war, weil das Passwort abgelaufen war. Wenn zudem keine starke Authentifizierung vorhanden war, mussten provisorische Umgehungsmöglichkeiten gefunden werden, die interne Schnittstellen ohne zusätzliche Sicherheitsebene der Öffentlichkeit zugänglich machten.

SCHLÜSSELRATSCHLÄGE

A. BEKANNTE RISIKEN NEU BEWERTEN

- Erhöhte Bedrohungsexposition durch hastig eingerichtete Zugangspunkte für den Fernzugriff. Sobald diese Tatsache bekannt wird, könnten sich die Kriminellen zusätzlich auf die Suche nach Exploits konzentrieren, was die Bedrohungslandschaft noch weiter vergrößert.

B. ZUSÄTZLICHE MAßNAHMEN ERWÄGEN

- Erwägen Sie, einen sicheren Fernzugrif in Zeiten einzurichten, in denen keine Krise herrscht.
- Systematische Einführung einer starken Authentifizierung (für alle kritischen Systeme und alle Mitarbeiter).
- Ziehen Sie in Betracht, hochmoderne Cloud-Lösungen mit starker Authentifizierung einzusetzen.

5 / HOME OFFICE

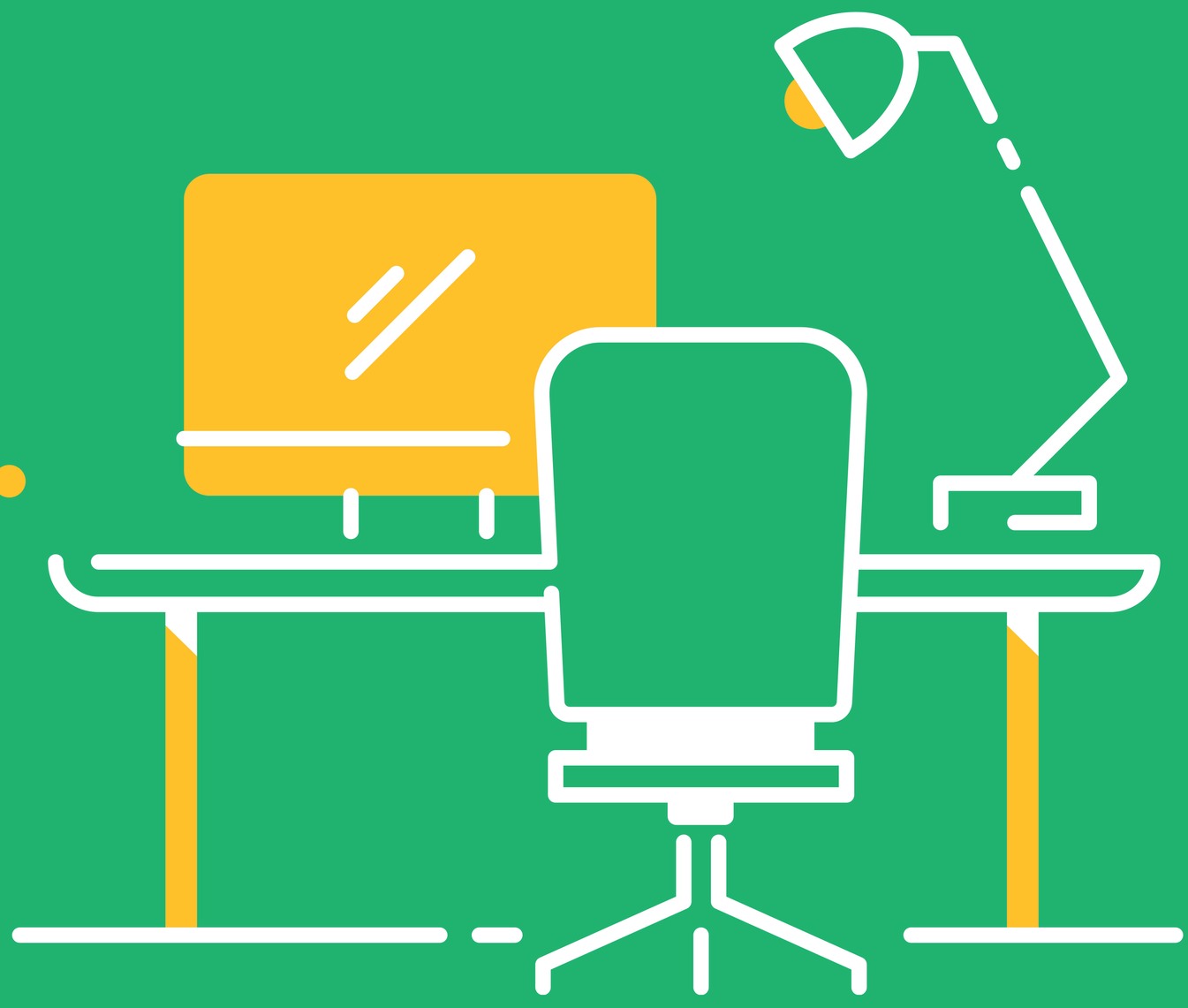
SCHLÜSSELERKENNTNISSE

Für jene Unternehmen, die die Möglichkeit hatten, aus der Ferne zu arbeiten, zeigte die Krise schnell ihre Grenzen auf.

- Erstens war nicht genügend Ausrüstung (seien es Laptops, Telefone oder Authentifizierungstokens) vorhanden, um sie an das gesamte Personal auszugeben.
- Zweitens bewältigte die Infrastruktur oder das Netzwerk selbst viele gleichzeitige Verbindungen nicht sehr gut.
- Drittens wurden nicht alle Arbeitsabläufe vollständig digitalisiert, so dass sie aus der Ferne nicht reibungslos fortgesetzt werden konnten.
- Viertens: Da die Krise die gesamte Wirtschaft traf, verzögerte sich die Beschaffung von starken Authentifizierungs-Token aufgrund der enormen Nachfrage weitgehend (ähnlich wie bei den Hygienemasken und Desinfektionsmitteln).

In einigen Fällen, insbesondere bei internationalen Konzernen verfügten nicht alle Arbeitnehmer über eine zuverlässige Internetverbindung, und 4G-Hotspots mussten vom Unternehmen bereitgestellt werden.

Das Arbeiten aus der Ferne schuf auch neue Sicherheitsprobleme. Zum einen stellt jede Person, die sich aus der Ferne verbindet, einen Zugangspunkt zu den internen Systemen dar und vergrößert damit die Angriffsfläche. Leider ist es sehr schwierig, diese Endpunktgeräte zu schützen, ganz zu schweigen von den Endpunktnetzwerken. Da zudem die gesamte interne Kommunikation nun über E-Mail erfolgte, wurden Phishing- und andere Social Engineering-Angriffe viel einfacher und effektiver.



Videokonferenzplattformen wurden bereits ausgiebig genutzt. Es stellte sich heraus, dass nicht alle von ihnen ausreichend sicher (z.B. fehlende Verschlüsselung) und daher für interne Sitzungen ungeeignet waren. Zudem wurden viele Fälle von Konferenzstürmungen (ungebetene Teilnehmer) gemeldet.

Im Allgemeinen hatten die Unternehmen nicht viele IT-Probleme bei den Endbenutzern, sondern setzten nur für den Fall der Fälle einen ständig besetzten IT-Support ein. Die meiste Hilfeleistung konnte per Fernzugriff über VPN bereitgestellt werden.

Wenn Mitarbeiter aus der Ferne arbeiten, waren die normalen Sicherheitsmaßnahmen (Anti-Virus, SIEM, Patching und Backup-Server) nicht unbedingt verfügbar, insbesondere wenn die Mitarbeiter keine Verbindung zum VPN herstellten. Daher waren alternative Lösungen erforderlich, wie z.B. die Zugänglichkeit der entsprechenden Dienste über das öffentliche Internet. Die Mitarbeiter wurden ermutigt, Cloud-Storage für die Speicherung ihrer Dateien zu nutzen – es war jedoch sehr schwierig, sicherzustellen, dass sie tatsächlich Cloud-Storage und nicht ihr lokales Dateisystem (das nicht gesichert wird) nutzten.

SCHLÜSSELRATSCHLÄGE

A. BEKANNTE RISIKEN NEU BEWERTEN

- Erhöhtes Risiko von Phishing und Social Engineering.
- Persönliche (nicht überwachte) Geräte sind an die internen Netzwerke angeschlossen. Sensible Daten können unter Umständen den Unternehmensbereich verlassen.
- Die Kommunikation zwischen den Mitgliedern des Unternehmens erfolgt meist über das Internet.
- Erhöhtes Risiko eines Datenverlusts aufgrund nicht erstellter Backups.

B. BESTEHENDE SICHERHEITSMAßNAHMEN VERBESSERN

- Berücksichtigen Sie die Situation, in der die Telekommunikationsleitungen und die IT-Infrastruktur aufgrund der Anhäufung von Verbindungen erschöpft sein werden für (ziehen Sie Logdateien zur Vorbereitung eines Vorfalls zu Rate).

C. NEUE KRISENSPEZIFISCHE RISIKEN ERKENNEN

- Passen Sie das Sensibilisierungstraining an die neue Situation (Arbeit aus der Ferne) an.
- Komplexe Arbeitsabläufe überprüfen, um sie krisenfest zu machen.
- Stresstest der Fernzugangsinfrastruktur (nutzen Sie den Rest der Krise zu Testzwecken). Erwägen Sie den Erwerb von VDI-Lösungen (virtuelle Desktop-Infrastruktur).

D. ZUSÄTZLICHE MAßNAHMEN ERWÄGEN

- Digitalisieren Sie Prozesse durch die Einrichtung sicherer Cloud- und E-Signatur-Plattformen.
- Stellen Sie sicher, dass alle Mitarbeiter bei Bedarf aus der Ferne arbeiten können.
- Stellen Sie sicher, dass genügend Reserve-Authentifizierungstoken verfügbar sind.
- Lösung des Endpunktsicherheitsproblems (Bereitstellung von Unternehmensmaterial für Benutzer, die zu Hause arbeiten, um Datenschutzprobleme zu vermeiden und ein gewisses Maß an Sicherheit zu erwingen).
- Verbieten Sie Mitarbeitern ausdrücklich, ihre private E-Mail-Adresse für den Firmengebrauch zu verwenden.
- Unternehmen sollten in eine Open-Source-Plattform investieren, die in ihren Räumlichkeiten oder bei einem Dienstleister eines vertrauenswürdigen Unternehmens gehostet wird. Die Verschlüsselung von Konferenzsystemen sollte Standard sein, was zur Zeit leider noch nicht bei allen der Fall ist.

6 / CYBER-GEFÄHRDUNGSLAGE

SCHLÜSSELERKENNTNISSE

Zu Beginn der Krise zeigte sich, dass die Cyberkriminellen schnell darauf reagierten, dass die meisten Unternehmen, ob vorbereitet oder nicht, anfingen, aus der Ferne zu arbeiten. Vor allem Scam und Phishing, aber auch Lösegeldforderungen (Ransomware) waren schnell auf dem Vormarsch. In einigen Fällen wurden kleinere DDoS-Angriffe auf die Kommunikationsinfrastruktur beobachtet.

Dem erhöhten Risiko von (Phishing-) Angriffen zu begegnen, wurde eine spezielle Schulung zur Sensibilisierung durchgeführt. Zur Organisation der Schulung wurden Online-Lernplattformen genutzt.

SCHLÜSSELRATSCHLÄGE

A. BEKANNTE RISIKEN NEU BEWERTEN

- In einer unerwarteten Situation, wie z.B. einer Situation, die ihre Gesundheit bedroht, Mitarbeiter neugierig auf Neuigkeiten und Informationen. In dieser Situation ist es für Betrüger leicht, Menschen dazu zu bringen, gefährliche Anhänge zu öffnen.
- Gateways für den Fernzugriff sind zu Single Points of Failure geworden, die vor Verfügbarkeitsverlust geschützt werden müssen.
- Regierungsentscheidungen könnten sich auf die Verfügbarkeit von Personal auswirken (Sozialurlaub).
- Geopolitische Spannungen.

B. BESTEHENDE SICHERHEITSMAßNAHMEN VERBESSERN

- Schlüsselpersonen müssen auch dann verfügbar bleiben, wenn sie ein Recht auf Urlaub haben (z.B. Sozialurlaub). Diese Schlüsselpersonen müssen hochgradig engagiert und dem Unternehmen gegenüber loyal und motiviert sein. Sehen Sie die Möglichkeit vor, für ihre Kinder zu sorgen, indem Sie vor Ort Kinderbetreuung anbieten.
- Stärkung des Sicherheitsbewusstseins mit Schwerpunkt auf Social Engineering.

C. ZUSÄTZLICHE MAßNAHMEN ERWÄGEN

- Informieren Sie die Mitarbeiter kontinuierlich über die Situation, und machen Sie sie auf Betrügereien aufmerksam.
- Sehen Sie DDoS-Minderungstechniken oder robustere Infrastrukturen vor.
- Seien Sie in der Lager, einen Cyber-Zwischenfall auch in Krisenzeiten zu bewältigen, d.h. auch dann, wenn die Ressourcen vor Ort nicht schnell verfügbar sind.

FEDIL erinnert Sie daran, dass die Cybersecurity-Checkliste betreffend Geräte, E-Mails, Zugriff auf die Cloud und das Netzwerk sowie Videokonferenzen in Zusammenarbeit mit SECURITYMADEIN.LU auf der FEDIL-Webseite verfügbar ist: Cybersecurity Checklist

Wenn Sie IND-ISAC beitreten möchten, kontaktieren Sie bitte:

Céline Tarraube
Adviser Digital & Innovation
celine.tarraube@fedil.lu
(+352) 43 53 66 610