NOTFALLPROTOKOLL BEI CYBERANGRIFFEN

Im Zeitalter der Digitalisierung ist die Bedrohung durch Cyberangriffe allgegenwärtig. Alle Unternehmen, vom kleinsten bis zum multinationalen Konzern, können ins Visier genommen werden. Laut einem ENISA-Bericht aus dem Jahr 2021 haben fast 68 % der KMUs einen Cyberangriff erlebt. Angesichts dieser Tatsache wird es zu einer Priorität zu verstehen, wie man effektiv auf einen Cyberangriff reagieren kann. Hier erfahren Sie, wie Sie in diesen schwierigen Situationen vorgehen können:

Vorbereitung auf eine potenzielle Cyberattacke

- **Identifizierung der Systeme.** Erstellen Sie ein vollständiges Inventar aller Geräte und Systeme (Server, Desktops, Laptops, Tablets, Smartphones, etc.), die mit Ihrem Netzwerk verbunden sind. Dies wird Ihnen einen Überblick über Ihre gesamte Infrastruktur verschaffen.
- **Sicherung von Daten.** Stellen Sie sicher, dass Sie über gesicherte Kopien aller wichtigen Daten verfügen. Nutzen Sie Online-Backup-Dienste oder externe Festplatten, um die Wiederherstellung im Falle eines Verlustes zu gewährleisten.
- **Netzwerkschutz.** Installieren Sie eine robuste Firewall und stellen Sie sicher, dass alle Ihre Systeme und Software regelmäßig aktualisiert werden, um Schwachstellen aufzuheben.
- **Schulung der Mitarbeiter.** Führen Sie Schulungen durch, um Ihre Mitarbeiter über die verschiedenen Cyberbedrohungen aufzuklären und ihnen gute Praktiken zur Vermeidung von Vorfällen zu vermitteln.
- **Reaktionsplan im Falle eines Cyberangriffes.** Erstellen Sie einen detaillierten Plan, der die genauen Schritte beschreibt, die im Falle eines Sicherheitsvorfalls zu befolgen sind.

So reagieren Sie richtig!

- **Identifizierung.** Achten Sie auf Anzeichen eines möglichen Angriffs, wie z.B.:
  - Unerwartete Verbindungsprobleme
  - Unerlaubte Änderungen an Dateien
  - Abnormales Systemverhalten
  - etc.
- **Bleiben Sie ruhig.** Auch in Krisensituationen ist es wichtig, ruhig zu bleiben und sich an die festgelegten Verfahren zu halten.
- **Informieren Sie Ihren Vorgesetzten.** Kommunizieren Sie schnell mit Ihrem Vorgesetzten und geben Sie ihm genaue Details über den Vorfall.
  - **Seien Sie präzise.** Geben Sie konkrete Informationen über Ihre Beobachtungen: betroffene Systeme, Warnungen (oder Hinweise), den Zeitpunkt der ersten Entdeckung, etc.
  - **Versuchen Sie nicht eine Lösung zu finden.** Versuchen Sie nicht die Malware zu entfernen oder die Systeme selbst wiederherzustellen, es sei denn, Sie sind ein Experte für Cybersicherheit.
  - **Folgen Sie den Anweisungen.** Nachdem Sie Ihren Vorgesetzten informiert haben sollten Sie bereit sein seinen Anweisungen zu folgen.
  - **Dokumentieren Sie Ihre Handlungen.** Führen Sie ein Protokoll Ihrer Handlungen und jedes von Ihnen beobachtete ungewöhnliche Verhalten.

  Ihre prompte Meldung kann bei der Bewältigung eines Cyberangriffs einen großen Unterschied machen.
- **Dämmen Sie den Angriff ein.** Führen Sie die folgenden Schritte aus, um die Auswirkungen des Cyberangriffs zu bewältigen und einzuschränken:
  - **Handeln Sie schnell**, um die Auswirkungen des Angriffs zu begrenzen.
  - **Trennen Sie kompromittierte Systeme vom Netzwerk**, um die Ausbreitung des Angriffs zu verhindern.
  - **Erstellen Sie mit professioneller Hilfe Notfall-Backups**, falls Sie nicht bereits über solche verfügen.

    Zu den Methoden können gehören:
    - Nutzung eines Online-Backup-Dienstes (Cloud);
    - Speichern von Kopien wichtiger Dateien auf einer externen Festplatte.

  Seien Sie sich des Risikos bewusst, das mit der Sicherung von Daten während eines Angriffs verbunden ist.

- **Kontaktieren Sie einen Experten.** Wenn Sie sich nicht sicher sind oder der Vorfall zu schwerwiegend ist, kontaktieren Sie einen Experten für Cybersicherheit. Das Computer Incident Response Center Luxembourg (CIRCL) ist zum Beispiel eine wertvolle Ressource.
  - Tel.: (+352) 247 88444
  - E-Mail: info@circl.lu

  Seien Sie bereit so viele Informationen wie möglich über den Vorfall zu liefern, einschließlich:
  - der Art des Angriffs;
  - der betroffenen Systeme;
  - der kompromittierten Daten;
  - der Maßnahmen, die Sie bislang ergriffen haben, um den Angriff einzudämmen;
  - etc.

Es ist wichtig, ein Ereignisprotokoll mit allen Beschreibungen, Beweisen und der Chronologie zu führen, auch wenn nicht alle diese Informationen sofort verfügbar sind. Diese Informationen werden den Fachleuten helfen, die Situation zu verstehen und die besten Schritte zu bestimmen.

Aktivitäten nach einem Zwischenfall

Bewertung des Angriffs. Sobald die Bedrohung eingedämmt ist, sollten Sie sich die Zeit nehmen, das Ausmaß des Schadens zu bewerten. Identifizieren Sie die betroffenen Systeme und bestimmen Sie die Art der potenziell gefährdeten Daten. Suchen Sie nach verräterischen Hinweisen, wie z.B.:

- Verbindungsproblemen
- Unerklärliche Änderungen an Dateien
- Unregelmäßige Systemleistung
- Warnungen von Sicherheitssoftware
- etc.

- **Benachrichtigung.** Informieren Sie alle betroffenen Parteien über den Vorfall, seien es Kunden, Partner oder Regulierungsbehörden (z.B. die nationale Datenschutzkommission (CNPD) oder die Polizei).
- **Behebung und Wiederherstellung.** Arbeiten Sie an der Wiederherstellung Ihrer Systeme. Dies kann die Bereinigung infizierter Systeme oder die Wiederherstellung aus Sicherungen erfordern.
- **Analyse nach einem Vorfall.** Überlegen Sie, was den Vorfall verursacht haben könnte. Identifizieren Sie Sicherheitslücken, verstärken Sie Ihren Schutz und bewerten Sie Ihre aktuellen Verfahren neu, um zukünftige Vorfälle zu vermeiden.

Schluss-folgerung

Cybersicherheit ist nicht nur eine Frage der Technologie, sondern auch der Aufklärung und der Vorbereitung. Die Investition in robuste Sicherheitsmaßnahmen, die regelmäßige Schulung Ihrer Mitarbeiter und ein klarer Aktionsplan für den Fall eines Vorfalls sind von entscheidender Bedeutung. Für Unterstützung und Beratung steht Ihnen der NC3 in Luxemburg zur Verfügung.

Für zusätzliche Informationen zum Notfallprotokoll bei Cyberangriffen:

CHAMBRE DES MÉTIERS LUXEMBOURG

Haben Sie noch Fragen?
Möchten Sie weitere Informationen zu den bestehenden Angeboten erhalten? Kontaktieren Sie die Abteilung eHandwierk der Chambre des Métiers:

E-Mail: **ehandwierk@cdm.lu**

Tel.: **42 67 67 - 505**