Cyberdelikte verhindern

Wegleitung für kleine und mittlere Unternehmen

Impressum

Kantonspolizei Bern und Melde- und Analysestelle Informationssicherung MELANI im Auftrag von Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK). Kontakt: Kantonspolizei Zürich, NEDIK, Zürich, cyc_nedik@kapo.zh.ch

Bilder: Von der Kantonspolizei Zürich zur Verfügung gestellt.

Ihre **POLIZEI**
Votre **POLICE**
La vostra **POLIZIA**

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

Inhaltsverzeichnis

1 Cyberangriffe kosten Geld, auch Sie?

Die Digitalisierung eröffnet der Wirtschaft neue Wachstumschancen und Beschäftigungsmöglichkeiten. Allerdings bedeutet dies auch eine zunehmende Abhängigkeit von einer funktionierenden IT-Infrastruktur. Dies nutzen Kriminelle aus. Vom Handwerksbetrieb bis zu grossen Firmen mit mehreren Tausend Mitarbeitenden – es kann alle treffen. Gemäss einer Untersuchung wurden bereits rund 40 Prozent der befragten Schweizer Unternehmen Opfer von Cyberkriminalität.[1] Dabei könnte nicht nur die Website offline gehen, sondern das gesamte Netzwerk eines Unternehmens betroffen sein. Meist erleiden Unternehmen finanzielle Schäden und in manchen Fällen können auch vertrauliche Informationen an die Öffentlichkeit gelangen.

Vor vielen Cybergefahren kann man sich schützen.

Mit diesem Informationsmaterial geben die Polizei und die Melde- und Analysestelle Informationssicherung (MELANI) konkrete Empfehlungen zum Schutz vor Cyberkriminalität und zeigen auf, wie bei einem erfolgten Angriff vorgegangen werden kann. Zudem wollen wir Sie dazu ermutigen, wenn Sie von relevanten Vorfällen betroffen sind, diese bei der Polizei anzuzeigen. Denn nur durch einen Schulterschluss von Strafverfolgungsbehörde und Wirtschaft können Täter/-innen ermittelt, verurteilt und so Cyberkriminalität nachhaltig bekämpft werden.

Vertiefte Informationen zu Ihrer IT-Sicherheit finden Sie auf www.melani.admin.ch

1 «Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse», PwC, 2018.

2 Wie Cyberangreifer/-innen an Ihr Geld kommen

Bei Cyberangriffen geht die Täterschaft oft nach denselben Mustern vor und verwendet immer wieder dieselben Mittel. Diese lassen sich grob in die Kategorien Erpressung, Betrug und Datenmissbrauch aufteilen.

2.1 Wie sie Sie erpressen

Die Erpresser/-innen greifen die Informatikinfrastruktur der Opfer mit dem Ziel an, Geld zu erpressen. Dabei werden möglichst viele Prozesse im Unternehmen gestört oder sogar gestoppt. Die Opfer werden kontaktiert und sollen einen bestimmten Betrag bezahlen, damit der Angriff aufhört oder gestohlene Daten nicht veröffentlicht werden.

Die Angreifer/-innen kennen Art und Grösse der Unternehmen, die sie attackieren.

Ransomware	Schädlinge werden grossflächig verschickt, zum Beispiel per E-Mail, um Informationen und Passwörter zu stehlen. Die mit dieser Methode gefundenen Opfer werden im Anschluss gezielt ausgespäht und es werden Informationen gesammelt. Hat die Täterschaft Erfolg, übernimmt sie die Kontrolle und beginnt die Firmendaten zu verschlüsseln. Gegebenenfalls werden auch Daten gestohlen. Die Erpresser/-innen fordern ein Lösegeld (engl. Ransom), damit die Daten wieder entschlüsselt werden können.
DDoS (Überlastattacken)	Ein vom Internet her erreichbares System wird durch sehr viele Anfragen überlastet, sodass die eigentliche Aufgabe nicht mehr wahrgenommen werden kann. Damit der Angriff aufhört, soll ein Lösegeld bezahlt werden. Täterschaften können aber auch Gruppierungen sein, die dem Unternehmen oder der Organisation schaden wollen, oder Konkurrenten/-innen, die sich einen Marktvorteil verschaffen möchten.
Veröffentlichung von Daten	Die Erpresser/-innen drohen, Daten, welche zuvor vom Unternehmen gestohlen wurden, zu veröffentlichen, falls kein Lösegeld bezahlt wird.

2.2 Wie sie Sie betrügen

Die Betrüger/-innen versuchen die Opfer durch Täuschung dazu zu bringen, etwas zu tun, was diese eigentlich nicht wollen. Oftmals wird dabei ein Szenario gewählt, welches möglichst viele Emotionen bei der Zielperson weckt oder ihnen vertraut ist. Die Vertrautheit verleitet zu einem falschen Sicherheitsgefühl.

Die Täterschaft informiert sich im Vorfeld vielfach über die Struktur des Unternehmens. Dies geschieht durch verfügbare Informationen (zum Beispiel auf der Website des Unternehmens oder in sozialen Netzwerken). Daraufhin wird eine Zielperson ausgesucht und diese mit einem auf sie zugeschnittenen Szenario konfrontiert. Die Methode, welcher sich die Täterschaft bedient, heisst Social Engineering. Mit Social Engineering soll erreicht werden, dass die Opfer die von der Täterschaft gesteuerten Handlungen ausführen, ohne es zu bemerken.

Hierarchie	Die Täterschaft nutzt den hierarchischen Aufbau eines Unternehmens aus und baut einen gewissen Handlungsdruck auf. Beispielsweise täuscht sie eine Identität vor und fordert einen Mitarbeiter oder eine Mitarbeiterin im Namen einer vorgesetzten Person auf, sensible Informationen freizugeben oder eine Geldüberweisung vorzunehmen.
Zeitdruck	Den Opfern wird vorgegaukelt, unter Zeitdruck handeln zu müssen.
Gier / Neugier	Dem Opfer wird ein Gewinn oder eine Überraschung versprochen, wenn die Datei geöffnet wird oder auf den Link geklickt wird.
Angst / Wut	Es wird mit Konsequenzen gedroht, falls der Aufforderung nicht nachgekommen wird. Oder es werden offensichtlich falsche Aussagen gemacht, die man mit einem Klick auf den Link bereinigen soll.
Anteilnahme	Das präsentierte Thema spricht das Opfer emotional an. Das Opfer will sich zum Beispiel beteiligen, um Missstände zu beseitigen.

2.3 Wie sie Ihre Daten missbrauchen

Oft wird durch Schadsoftware vom Konto der Opfer Geld abgehoben. Aber auch mit gestohlenen Zugangsdaten kann durch den Verkauf auf dem Schwarzmarkt Geld verdient werden.

Zum Teil sind auch gewinnbringende Firmendaten Ziel des Vorhabens. Hierbei handelt es sich vorwiegend um Geschäftsgeheimnisse oder Kundendaten. Falls Ihre Firma Zugangsdaten von Kunden oder sogar Kreditkartendaten speichert, sind diese von grossem Interesse für Kriminelle.

Die Daten sollten speziell gesichert (verschlüsselt) aufbewahrt werden.

E-Banking-Trojaner	E-Banking-Trojaner sind Programme, welche den Angreifenden einen Zugang auf Ihr E-Banking-Konto ermöglichen. Trojaner werden oft per E-Mail versandt (zum Beispiel getarnt als Rechnung oder Bewerbung).
Datenabfluss	Die Angreifer/-innen verschaffen sich Zugang auf Ihr Unternehmensnetzwerk. Finden sie wertvolle Daten, werden diese kopiert. Anschliessend können sie entweder an Dritte verkauft werden oder die Firma wird mit der Drohung der Herausgabe erpresst.
Phishing	Phishing ist eine Technik, um an vertrauliche Daten zu gelangen. Sie findet zum Beispiel per E-Mail, Website, Internettelefonie oder Kurznachricht statt. Die Empfänger/-innen werden darauf hingewiesen, dass Zugangsdaten nicht mehr sicher oder aktuell seien und man diese unter dem aufgeführten Link ändern solle. Der Link führt jedoch auf eine gefälschte Website. Die Opfer loggen sich ein. Damit erhält die Täterschaft die Zugangsdaten und kann zum Beispiel Waren auf Rechnung bestellen.

3 Wie Sie Ihr Unternehmen schützen können

Um einen Angriff zu vermeiden, braucht es technische und organisatorische Massnahmen. Diese lassen sich nicht an Mitarbeitende delegieren, sondern müssen von der Geschäftsleitung angegangen und koordiniert werden.

Massnahmen gegen Cyberangriffe müssen von der Geschäftsleitung angegangen werden.

3.1 Mit technischen Schutzmassnahmen

> **Nehmen Sie Sicherheitsupdates vor**
Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Stellen Sie sicher, dass sämtliche Computer und Server in Ihrem Netzwerk Sicherheitsupdates automatisch einspielen. Bringen Sie auch Drittsoftware wie zum Beispiel Adobe Reader, Adobe Flash und Java regelmässig auf den neuesten Stand. Das gilt auch für Geräte wie Drucker, Router usw.

Falls Ihr Unternehmen über einen Webauftritt verfügt, stellen Sie sicher, dass ein gegebenenfalls eingesetztes Content Management System (CMS), also das Websiteverwaltungssystem, stets auf dem aktuellsten Stand ist. Die meisten CMS bieten eine einfach zu aktivierende, automatische Updatefunktion an.

> **Schützen Sie Ihr Netzwerk**
Verwenden Sie eine Firewall: Auf jedem Computer sollten Sie eine Personal Firewall verwenden. Schützen Sie zudem Ihr Unternehmensnetzwerk mit einer Firewall vor dem Internet. Standardmässig sollte die Firewall sämtlichen Verkehr blockieren, ausser den durch Regeln freigegebenen Datenverkehr.

Unterteilen Sie Ihr Unternehmensnetz in einzelne Bereiche. Zum Beispiel: je ein separates Netz für Produktion, Personal und Buchhaltung. Es gibt keinen Grund, weshalb Mitarbeitende des Personaldienstes auf Ihre Produktionsanlage zugreifen sollten. So vermeiden Sie, dass beispielsweise Steuerungscomputer von Werksanlagen, die nicht mehr aktualisiert werden können, zum Einfallstor für Angreifende werden.

Sichern Sie Ihren Fernzugriff: Schützen Sie Fernzugriffe auf Ihr Netzwerk keinesfalls mit einer einfachen Authentisierung (Benutzername und Passwort). Nutzen Sie mindestens eine Zwei-Faktor-Authentisierung oder setzen Sie eine sicherere Verbindung über ein virtuelles privates Netzwerk (VPN) ein. Dies gilt auch für den Zugriff von externen IT-Dienstleistern und Administratoren.


PASSWORD

> **Sichern Sie Ihre Daten**
Definieren Sie einen Prozess, der die regelmässige Datensicherung regelt, und halten Sie diesen konsequent ein. Überlegen Sie sich, wie viele Tage Datenverlust Sie verkraften können, und lagern Sie entsprechend eine zusätzliche Kopie Ihres Back-ups getrennt (offline) und ausser Haus (offsite) aus. Üben Sie von Zeit zu Zeit das Einspielen von Back-ups, sodass Sie mit dem Prozess vertraut sind, wenn Sie einmal darauf angewiesen sein sollten. Stellen Sie sicher, dass Sie Vorgängerversionen des Back-ups über einen mehrmonatigen Zeitraum aufbewahren.

> **Installieren Sie einen Virenschutz**
Stellen Sie sicher, dass auf jedem Computer ein Virenschutz installiert und der Echtzeitschutz aktiviert ist. Sorgen Sie auch dafür, dass dieser sich regelmässig aktualisiert sowie täglich einen vollständigen Systemscan durchführt.

> **Vorsichtiger Umgang mit Clouddiensten**
Seien Sie vorsichtig bei der Verwendung von Clouddiensten. Diese werden von vielen Programmen verwendet. Überlegen Sie sich, welche Daten lokal und welche in der Cloud gespeichert werden sollen. Sensible Daten und Firmengeheimnisse sollten nie unverschlüsselt in der Cloud abgelegt werden.

Vorsorge ist wichtig!
Machen Sie sich im Vorfeld Gedanken, welche Massnahmen bei einem Angriff getroffen werden müssen. Definieren Sie, welche Logdateien (Ereignisprotokolldateien) gespeichert werden und wie lange. Computer und Server können alle systemrelevanten Vorgänge oder Verbindungsdaten zu anderen Computern aufzeichnen. Am besten geschieht dies an einem zentralen Ort. Umfangreiche Logdaten helfen nicht nur den Strafverfolgungsbehörden bei ihren Ermittlungen, sondern auch den Unternehmen, den Ursprung eines Angriffs zu erkennen, Informationen über infizierte Systeme im eigenen Netzwerk zu erhalten und geeignete Gegenmassnahmen zu ergreifen. Sollte Ihr Netzwerk durch ein IT-Dienstleistungsunternehmen administriert werden, empfehlen wir Ihnen, Fragen zu Logdateien und der Detektion von Angriffen mit diesem zu klären. Es ist ebenfalls zu empfehlen, einen aktuellen und vollständigen Bestand aller Systeme, Software und Netzwerke zu führen.

3.2 Mit organisatorischen Schutzmassnahmen

> **Regeln Sie den Umgang mit Unternehmensinformationen**
Definieren Sie Richtlinien zur Weitergabe von Unternehmensinformationen. Überlegen Sie genau, welche Informationen Sie zum Beispiel auf der eigenen Website oder in sozialen Medien offenlegen, da diese von Kriminellen gesammelt werden. Über anonyme Kanäle (zum Beispiel Telefon oder E-Mail) sollten grundsätzlich keine vertraulichen Informationen weitergegeben werden.

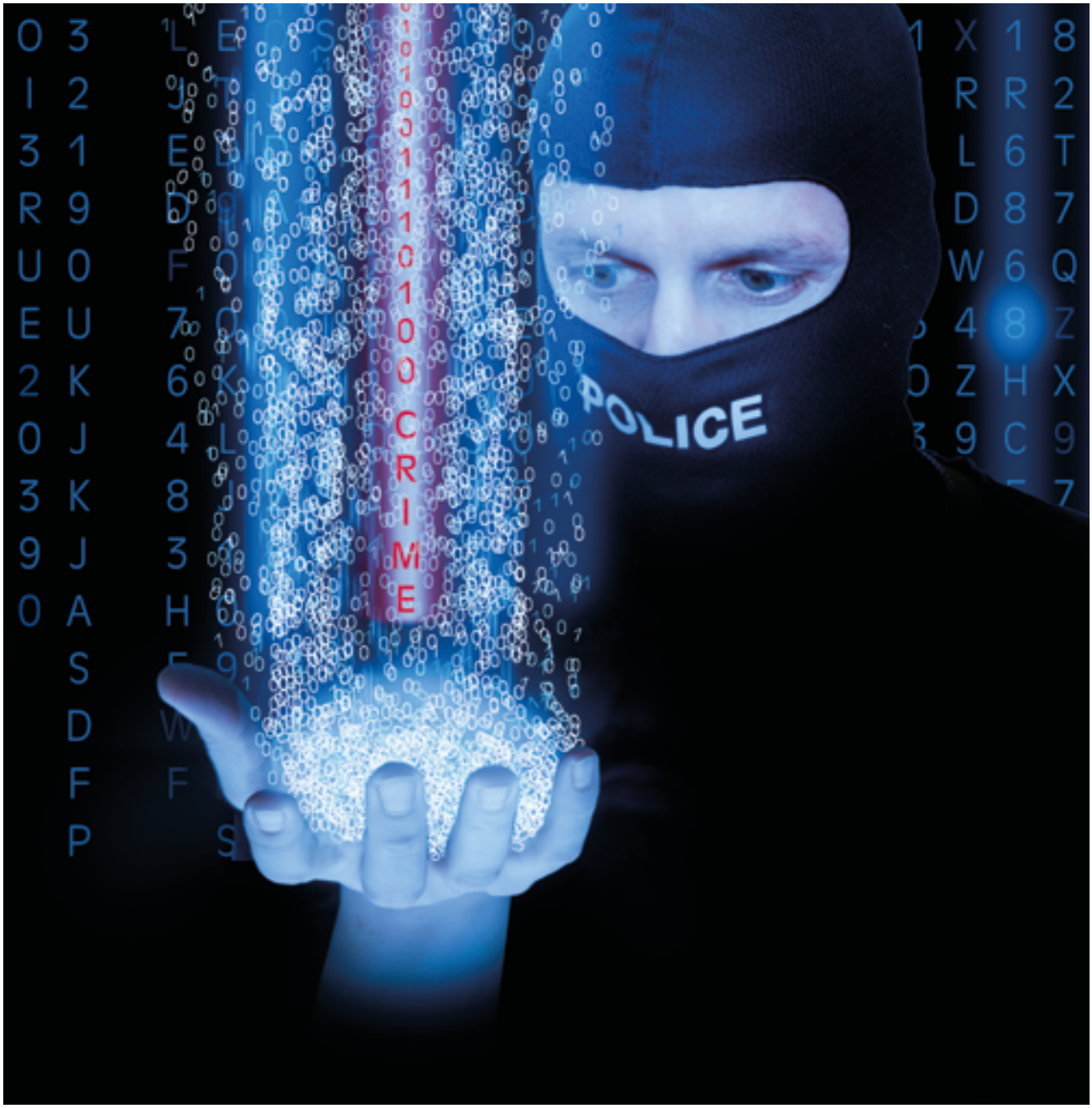
> **Sensibilisieren Sie Ihre Mitarbeitenden im Umgang mit E-Mails**
Häufig gelangen elektronische Schädlinge durch Anhänge getarnt als angebliche Rechnungen auf Ihren Computer. Haben Sie ein gesundes Misstrauen; scheuen Sie sich nicht vor einer telefonischen Rückfrage und sensibilisieren Sie auch Ihre Mitarbeitenden. Stellen Sie unbedingt sicher, dass keine Makros in Microsoft-Dokumenten unsicherer Herkunft ausgeführt werden können.

> **Verwenden Sie sichere Passwörter und geben Sie diese nicht weiter**
Definieren Sie verbindliche Passwortregeln und setzen Sie diese konsequent durch. Die Mindestlänge des Passwortes sollte bei zwölf Zeichen liegen und sowohl aus Buchstaben, Zahlen wie auch Sonderzeichen bestehen. Setzen Sie wo immer möglich auf eine Zwei-Faktor-Authentisierung. Vermeiden Sie unbedingt die Mehrfachverwendung von gleichen Passwörtern! Stattdessen benutzen Sie einen Passwortmanager und generieren Sie für jede Anwendung ein eigenes Passwort. Sie finden auf dem Markt unterschiedliche Passwortmanagement-Systeme für die verschiedenen Betriebssysteme und Geräte; es gibt sowohl kostenlose als auch lizenzpflichtige Programme. Geben Sie Passwörter und Zugangsdaten niemals per Telefon oder E-Mail weiter.

> **Regeln Sie den Zugriffsschutz auf Daten**
Mitarbeitende sollten standardmässig über keine Administratorenrechte verfügen. Es gilt, Mitarbeitenden nur diejenigen Rechte zu gewähren, welche sie für die Ausführung der ihnen aufgetragenen Arbeit benötigen.

> **Schützen Sie Ihr Online-Bankkonto**
Verwenden Sie für Zahlungen einen separaten Computer, auf welchem Sie nicht im Internet surfen oder E-Mails empfangen. Sämtliche Prozesse, welche den Zahlungsverkehr betreffen, sollten firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen eingehalten werden, zum Beispiel Vier-Augen-Prinzip und Kollektivunterschrift. Dabei müssen Zahlungen vor der Auslösung zusätzlich von einem/einer anderen E-Banking-Nutzer/-in visiert werden. Dies gilt insbesondere, wenn mehrere Mitarbeitende zahlungsberechtigt sind. Sprechen Sie mit Ihrer Bank über mögliche Sicherheitsmassnahmen.

> **Zusammenarbeit mit einem IT-Dienstleistungsunternehmen**
Während grössere Unternehmen häufig über eigene IT-Abteilungen verfügen, lagern viele kleinere diese Aufgaben aus. Stellen Sie sicher, dass die Zuständigkeiten zwischen Ihnen und dem IT-Dienstleistungsunternehmen bezüglich IT-Sicherheit klar geregelt sind. Dies betrifft insbesondere die oben beschriebenen technischen und organisatorischen Massnahmen. Legen Sie vertraglich fest, wie die Haftung in einem Schadenfall geregelt ist, wenn vereinbarte Sicherheitsmassnahmen nicht eingehalten wurden.


POLICE
CRIME

4 Wie auch Sie zur erfolgreichen Ermittlung der Täterschaft beitragen können

4.1 Jede Meldung ist entscheidend

Die Polizei ist nicht an Ihren Geschäftsgeheimnissen interessiert und wirkt nicht auf Ihre Infrastruktur ein. Sie sucht bei einem Angriff nur nach Informationen und Spuren, die für die Aufklärung der Straftat relevant sind. Die Untersuchung unterliegt dem Amtsgeheimnis. Befürchtungen über negative Auswirkungen bei der Erstattung einer Anzeige, beispielsweise die Sicherstellung von Firmenrechnern über eine längere Zeit oder die Veröffentlichung eines Falles, sind unbegründet. Die Polizei nimmt Sie sehr ernst und spricht in der Regel Strafverfolgungsmassnahmen zuerst mit den Firmen ab. In den meisten Fällen kann eine Vorgehensweise gefunden werden, welche für beide Seiten funktioniert.

Ermittlungen im Cyberbereich sind zwar herausfordernd, unter anderem auch, weil in vielen Fällen eine internationale Täterschaft dahintersteckt. Sie bringen aber auch Erfolge. Die Erfahrung zeigt, dass viele Straftaten im Cyberbereich zusammenhängen und Gemeinsamkeiten haben. Jede Anzeige kann deshalb den entscheidenden Hinweis zu einer Täterschaft liefern.

4.2 Melden Sie den Vorfall umgehend

Nach einer Straftat sollten Sie möglichst schnell die Polizei oder die Staatsanwaltschaft informieren. Je länger Sie warten, umso grösser ist die Wahrscheinlichkeit, dass wertvolle Spuren verwischt werden. Ausserdem kann jede Einwirkung dazu führen, dass Spuren nicht mehr verwendet werden können oder gelöscht werden. Jeder Polizeiposten nimmt eine Strafanzeige mündlich oder schriftlich entgegen. Auf dem Suisse-ePolice-Online-Portal www.suisse-epolice.ch finden Sie die Telefonnummer eines Polizeipostens in Ihrer Nähe.

4.3 Vorgehen bei einer Meldung ohne Strafanzeige

In einigen Fällen kann es sein, dass Firmen auf eine Anzeige verzichten. In diesem Fall haben die Behörden eine Möglichkeit geschaffen, dass Geschädigte Informationen an die Behörden zur Kenntnis weiterleiten können. Senden Sie hierzu eine Meldung an MELANI, www.melani.admin.ch. Für die Behörden ist es dank diesen Informationen möglich, eine bessere Übersicht über die aktuelle Bedrohungslage und ähnliche oder gleich gelagerte Straftaten zu erhalten sowie die Dunkelziffer der nicht gemeldeten Fälle zu verkleinern. Diese Hinweise können jedoch nicht für eine Anklage respektive in einem Gerichtsverfahren verwendet werden.

5 Was Sie tun müssen, wenn es trotzdem passiert

Erste Hilfe bei einem Cyberangriff
Trotz aller Vorsichtsmassnahmen kann es sein, dass Sie Opfer eines Cyberangriffs werden. Daher ist es wichtig, dass Sie wissen, was in einem solchen Fall zu tun ist.

1. Isolieren
   > Trennen Sie alle Systeme umgehend vom Netzwerk. Vergessen Sie nicht, das WLAN auszuschalten.
   > Warten Sie mit dem Wiederaufsetzen der Systeme, bis die Polizei die Spuren gesichert hat.

2. Kontaktieren
   > Kontaktieren Sie umgehend die Polizei. Spezialisierte Mitarbeitende beraten und unterstützen Sie im Vorgehen, sichern Spuren und ermitteln. Auf www.suisse-epolice.ch finden Sie die Telefonnummer eines Polizeipostens in Ihrer Nähe.
   > Spezialisierte privatwirtschaftliche Unternehmen helfen Ihnen, Ihre Infrastruktur zu reparieren und gegebenenfalls wiederherzustellen.
   > Melden Sie Angriffsversuche ohne Schaden bei MELANI.


JDF LOR9 D9AA9Q3O
HJO JU9UO FOSD2A2I
E3A DWEU 70OIOPOE
WL SE2K 6KLJIJ1U
L3 J80J 4LQAODSO
3L F 3K 8J2SJSJ2
KS 3 9J 319U1 A3
HD S 0A H01DL L9
F0 6 S E9LAH SO
HE L D W07JW K1
D3 0 F FDJ J J