Bundesministerium
Inneres

Bundeskriminalamt

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

WIE ERSTATTE ICH ANZEIGE

Tipps und richtiges Verhalten

IMPRESSUM

Medieninhaber/Verleger:
Fachverband Unternehmensberatung, Buchhaltung und IT der Wirtschaftskammer Österreich in Kooperation mit dem BM.I, Bundesministerium für Inneres |
Wiedner Hauptstrasse 63 | 1045 Wien |
Telefon: +43 5 90 900 3540 | E-Mail: ubit@wko.at

1. Auflage, Juli 2022

Für den Inhalt verantwortlich:
MR Ing. Mag.(FH) Andreas Mitak, Harald Wenisch,
MR Mag.(FH) Gert SEIDL

Projekt Idee: Harald Wenisch

Layout: LUCID Design & Werbung
Fotos: BMI, Gerd PACHAUER / shutterstock
Druck: Wograndl Druck GmbH | Druckweg 1 | 7210 Mattersburg

VORWORT

In den letzten Jahren ist ein kontinuierlicher Anstieg im Bereich Cybercrime zu sehen. Zunehmend stehen auch Klein- und Mittelunternehmen (KMU) im Visier von Cyberkriminellen.

In der Praxis zeigt sich, dass Verantwortliche mit dem Mittel der Anzeige sich oft schwertun bzw. auf das Wissen aus Film und Fernsehen zurückgreifen. Gerade bei Cybercrime Delikten fehlt oft die nötige Hilfestellung, um einfach, rasch und vollständig den Anzeigenweg zu beschreiten.

Wir erklären, wie Sie am besten eine Anzeige bei Cybercrime Vorfällen machen und wie Sie richtig reagieren, wenn es einmal bei ihnen im Unternehmen zu so einem Vorfall kommt.

In der Partnerschaft zwischen Behörde und Wirtschaft wird Ihnen als UnternehmerIn mit Rat und Tat geholfen. Wir zeigen Ihnen auch welche Zuständigkeiten es gibt und wer die richtigen Ansprechstellen für die einzelnen Fälle sind.

Achtung: Wenn es um einen konkreten Notfall mit Angriff auf Leib oder Leben geht, dann rufen Sie den Polizeinotruf 133 an!

INHALTSVERZEICHNIS


POLIZEI

ERSTATTUNG EINER ANZEIGE BEI CYBERCRIME

EINLEITUNG

Wenn Sie Opfer von Cyber-Kriminalität geworden sind, möchten wir Sie dazu ermutigen, strafrechtlich relevante Vorfälle bei der Polizei tatsächlich anzuzeigen.

Warum ist ganz klar: Betroffene von Straftaten haben ein Recht auf strafrechtliche Verfolgung der Täter und können später in einem Zivilverfahren entstandene Schäden geltend machen.

Aber auch die Allgemeinheit profitiert on der Anzeige, z.B. wenn es um dem Wirtschaftsstandort Österreich geht. Über den Weg der Anzeige können daher auch vermehrte Angriffe auf gewisse Regionen oder Bundesländer deutlich wahrgenommen werden, bis hin zu Angriffen die gezielt einzelne Wirtschaftssektoren schädigen wollen.

Auf Seiten der Polizei wurden schon bisher bei einer gezielten Häufung von Kriminalitätsformen sogenannte SOKOs (Sonderkommissionen) gebildet, um zielgerichtet die Auswertung und Verfolgung zu beschleunigen. Als Beispiel im Cybercrime-Bereich kann hier die SOKO CLAVIS angeführt werden, die vor Jahren gebildet wurde um erfolgreich die Ausbreitung der Erpresser-Trojaner (Ransomware) zu vermeiden. Somit kann auch jede Bürgerin und jeder Bürger zur Bildung einer Sonderkommission über den Weg der Anzeige aktiv beitragen.

ERSTMASSNAHMEN

Setzen Sie vorerst keinerlei Maßnahmen, welche Veränderungen am Gerät, dem Systembetrieb oder den gespeicherten Daten herbeiführen können! Angreiferinnen und Angreifer könnten dabei feststellen, dass deren Aktivitäten bereits entdeckt wurden. Zudem könnten so weitere mögliche Ermittlungsschritte durch die Polizei vereitelt werden.

Durch das vorzeitige Einspielen von Sicherungskopien würden zum einen Spuren vernichtet werden und zum anderen könnten auch schon die Sicherungskopien durch Schadsoftware kompromittiert worden sein.

Verwenden Sie zur Kommunikation und Reaktion auf den Cybercrime-Vorfall grundsätzlich ein anderes Kommunikationsmittel oder System als das bereits infizier e System!

ERSTBEURTEILUNG EINES CYBERCRIME-VORFALLS

Nutzen Sie vor der Anzeigeerstattung, falls erforderlich, die kostenlose Cyber-Security-Hotline für WKO-Mitglieder und holen sich österreichweit die telefonische Erste Hilfe bei der **24h-Hotline** unter **0800 888 133**.

Bewahren Sie trotz allem Ruhe und machen Sie einen ersten Aktionsplan, wer Ihnen helfen kann und gehen Sie strukturiert vor.

Bereiten Sie sich auf die Beantwortung der folgenden Fragen vor:

- Welche **Systeme** sind auf welche Weise betroffen?

- Welche **Nachweise** haben Sie, dass widerrechtlich auf Dateien oder Protokolle zugegriffen wurde und diese erstellt, verändert, gelöscht oder kopiert wurden oder neue Nutzerkonten bzw. Nutzerrechte hinzugefügt oder geändert wurden?

- Existieren **Protokollinformationen**
  - zur Bestimmung von unmittelbaren Ausgangspunkten des Angriffs?
  - zu Serverkennungen von allenfalls stattgefundenen Datenübertragungen?
  - zur Identitätsbestimmung weiterer Geschädigter?

- Wurden durch die Angreifer **Programme** installiert **oder Daten auf das System** kopiert?

- Wurden **Datei- oder Konfigu ationsänderungen** vorgenommen?

- Wurden **Log-Einträge** oder gar ganze **Logdateien** gelöscht?

- Wurden wichtige **Schutzmechanismen** des Systems **deaktiviert** (z.B. Virenscanner) ?

Sollten Sie auf einen Cybercrime-Angriff noch nicht vorbereitet sein oder technisch nicht in der Lage sein der Polizei diese Auskünfte zu geben, können Sie auch das 3-stufige Be atungssystem der WKO nutzen:

1) **Die Cyber-Security-Hotline** 0800 888 133 hilft mit einfachen Erstmaßnahmen. Am Telefon können, aus verständlichen Gründen, aber keine technischen Ferndiagnosen oder rechtliche, wie präventive Hilfestellungen gegeben werden.

2) **Das Erstgespräch** mit einem Profi kann er olgen, wenn Sie zur Ersten Hilfe der Cyber-Security-Hotline zusätzliche Unterstützung benötigen. Das Callcenter stellt dann den Kontakt zu einem auf IT-Security und Cyberkriminalität spezialisierten Unternehmen der Experts Group IT-Security des Fachverbandes UBIT in Ihrer Nähe her. Sie werden für das Erstgespräch zur weiteren Analyse vom IT-Security-Unternehmen kontaktiert.

3) **Dringende Hilfe** vor Ort für notwendige Sofortmaßnahmen und Maßnahmen zur Wiederherstellung des Normalbetriebes müssten erforderlichenfalls direkt mit einem IT-Security Unternehmen vereinbart werden. Die Verrechnung nach Stundensätzen für die Tätigkeiten vor Ort erfolgen direkt mit dem Beratungsunternehmen.

Versicherungen und allenfalls weitere **Geschädigte** des Vorfalls benötigen Informationen zum befallenen System. Diese dienen zu Analysen von Schadenshöhen und Behebungskosten. Bedenken Sie, dass dazu für die notwendige Anzeigeerstattung die Polizei für Beweise und Ermittlungen auch **Kopien zu forensischen Zwecken** benötigt!

Erstellen Sie deshalb **vor der Wiederherstellung des Systems**, wenn nötig mit Unterstützung eines auf IT-Security spezialisierten Unternehmens, zunächst eine **identische Kopie (Image) des betroffenen Systems**. Diese Sicherung dient für spätere Analysen ebenso wie als Nachweis für den stattgefundenen Angriff. Achten Sie auch darauf, dass schriftlich festgehalten wurde, wann, was, von wem und mit welchen Methoden gesichert wurde. Gerade bei mehreren Systemen oder größeren Schadenslagen kann leicht der Überblick verloren gehen.

Diese Images und Datenkopien von Dateien, Verzeichnissen, Wechseldatenträgern, gelöschten Daten und Informationen im Speicher können bei der Identifizierung von ausgenutzten Schwachstellen, installierten Schadprogrammen, sowie bei der Rückverfolgung von Angreifern durchaus hilfreich sein.

Zur Beschreibung und Feststellung des anzuzeigenden Vorfalls legen Sie bitte (eventuell mit Ihrem IT-Security Unternehmen) ein **Ereignisprotokoll für die Anzeigeerstattung** an, welches folgende Punkte umfassen sollte:

GESICHERTE BEWEISMITTEL

- Sichern Sie bitte relevantes Datenmaterial, wie alle bereits bestehenden Protokolle bzw. Log- und Verkehrsdaten (lokal, auf zentralen Servern und Netzwerkgeräten wie Firewall udgl.), verdächtige Dateien wie beispielsweise Emails, Chat-Verläufe, Zahlungsbelege, Screenshots, digitale Fotos, Videos oder ähnliches. Wenn bestimmte Inhalte nicht abgespeichert werden können, erstellen Sie Screenshots oder fotografie en Sie den Bildschirm notfalls ab.

- Stellen Sie sicher, dass sich die Unterlagen und Daten, die Sie der Polizei zur Verfügung stellen, im Originalzustand befinden. Das bedeu et, dass an ihnen keine Manipulation, keine Ergänzungen oder ähnliches durchgeführt wurden. Bei E-Mails würde das bedeuten, diese nicht einfach weiterzuleiten, sondern die Original-E-Mail abzuspeichern und die gespeicherte Kopie als Anhang zu übermitteln.

- Häufig haben Sie auch selb t die Möglichkeit, bei den von Ihnen betroffenen Accounts, Informationen abzufragen, die für eine Täterausforschung notwendig sind. Exemplarisch sind dies IP-Adressen über widerrechtliche Zugriffe inklusive Zeitstempel, Logdaten und so weiter.

  Überprüfen Sie dazu am besten selbst, welche der für die Tathandlung relevanten Daten beim jeweiligen Account-Anbieter beziehungsweise Online Service Provider (Thema Cloud) gespeichert werden und für Sie zugänglich sind oder deren Bekanntgabe über diesen angefordert werden kann.

TATZEITRÄUME

- Daten und Uhrzeiten (einschließlich Zeitzonen), an denen relevante Ereignisse entdeckt wurden bzw. stattfanden. Die enthaltenen Uhrzeit- und Datumsangaben mit den Zeitzonen sind in korrekten Protokolleinträgen sehr wichtig, um einen Angreifer zurückzuverfolgen und ihn zu überführen.

- Wenn es sich um komplexere Tathandlungen handelt, dokumentieren Sie den Tathergang in chronologischer Weise und stellen Sie sicher, dass die Geschehnisse zeitlich richtig eingeordnet sind.

TATORTE

- Auch beim Cybercrime gibt es einen oder mehrere Tatorte, wie z.B. betroffene Firmensitze, Home-Offi e-Adressen, Cloudanbieter, etc...).

SACHVERHALTSDARSTELLUNG

- Namen, Daten, Uhrzeiten zu relevanten Kontaktaufnahmen, wie Telefonanrufe, E-Mails und andere Verbindungen (insbesondere verdächtige Sachverhalte, die z.B. Social Engineering betreffen)

PERSONEN- UND KONTAKTDATEN

- Identitäten jener internen, wie externen Personen, welche die Aufgaben im Zusammenhang mit dem Schadensfall bearbeiten (i.d.R. Administratoren, IT-Security-Beratungsunternehmen)

- eine Beschreibung von deren Aufgaben

- Ansprechpersonen und Entscheidungsträgerinnen und Entscheidungsträger.

TÄTIGKEITEN UND ZEITAUFWÄNDE

- Die Aufstellung von vorgenommenen Tätigkeiten und deren Zeitaufwände der involvierten Personen hilft ihnen zur Nachvollziehbarkeit und zur Analyse der Schadenshöhe für Versicherungen. Auch etwaige kurzfristig erfolgte Auftragserteilungen und Anschaffungen sollten Ihnen mit Belegen dokumentiert werden.

AUFZÄHLUNG BETROFFENER SYSTEME

- mit allen betroffenen Kennungen, Konten, Diensten, Daten und Netze sowie die genaue Art der Beeinträchtigung.

SCHÄDEN

- mit Angaben zu Art, Umfang und einer Abschätzung der monetären Schadenshöhen.

Informieren Sie alle im Vorfeld festgelegten relevanten Personen, Dienstleistungsbetriebe und Institutionen nur über geschützte und zuverlässige Kanäle und beschränken Sie aufgrund möglicher Insidertäterinnen und Insidertäter die Anzahl der benötigten Adressaten.

ANZEIGEERSTATTUNG UND POLIZEILICHE ZUSTÄNDIGKEITEN

Einen Cybercrime-Vorfall können Sie in der Regel in jeder Polizeidienststelle zur Anzeige bringen. Für eine Erstinformation dient auch die zentrale Meldestelle im Bundeskriminalamt (BK) unter der E-Mail: **against-cybercrime@bmi.gv.at**.

Eine formelle Anzeigeerstattung über die Meldestelle des BK ist nicht vorgesehen. In der Folge kann es sein, dass bei schwerwiegenden und überregionalen Fällen auch Bezirks-IT-Ermittler, das Landeskriminalamt oder das Cybercrime Competence Center C4 des Bundeskriminalamtes zur Bearbeitung herangezogen werden.

Stellen Sie die gesicherten Daten nach Absprache mit dem aufnehmenden Beamten in geeigneter Form zur Verfügung (beispielsweise über **https://cryptshare.bmi.gv.at** oder einen Datenträger, wie CD-ROM oder USB-Stick). Die Daten auch physisch auf einem Datenträger auszuhändigen ist wichtig für die weiteren Ermittlungen, um jeglichen Verlust von Spuren in den Systemen und Netzen zu vermeiden.

Optimalerweise haben sie auch eine Kopie der übergebenen Daten bei ihnen aufliegen damit sie in der Bearbeitungszeit weiterhin handlungsfähig bleiben und Kenntnis über Umfang und Art der übergebenen Daten haben.

Bitte haben Sie Verständnis dafür, dass Sie bei einem ersten Gespräch mit der Polizei nicht sofort die für das unmittelbare Cybercrime-Delikt spezialisierten Cybercrime-Expertinnen und -Experten treffen und deshalb in den meisten Fällen oft in einem zweiten Schritt an eine dafür spezialisierte Fachdienststelle weitergeleitet werden oder von dort Rückfragen erhalten. Ziel ist es, mit ihnen möglichst rasch Kontakt herzustellen und erste Maßnahmen einzuleiten.

Darüber hinaus kann Ihnen die Meldestelle für Cybercrime im Bundeskriminalamt professionelle Auskunft über die weitere Vorgehensweise bei Cybercrime-Vorfällen geben.

Beachten Sie, dass bei einem Angriff auf Unternehmen der kritischen Infrastruktur auch die Direktion für Staatsschutz und Nachrichtendienst (DSN) zuständig ist!

INFORMATIONSPFLICHTEN

Informieren Sie alle bereits im Vorfeld festgelegten relevanten Personen, Dienstleister und Institutionen (auch i.S.d DSGVO) nur über geschützte und zuverlässige Kanäle. Beschränken Sie aufgrund möglicher Insidertäterinnen und Insidertäter die Anzahl der benötigten Adressaten.

Bedenken Sie ihre Informationspflicht im Rahmen der EU-Datenschutz-Grundverordnung (DSGVO), die zeitnahe erfolgen muss.

Die DSGVO definiert eine Verletzung des Schutzes personenbezogener Daten" (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Als „data breach" kann daher z.B. ein Vorfall verstanden werden, durch den Unbefugten der Zugriff auf Daten möglich wird (z.B. Verlust eines Datenträgers, Hackerangriff ...). Dadurch kann den betroffenen Personen ein physischer, materieller oder immaterieller Schaden entstehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten, Identitätsdiebstahl oder –betrug, finanziel e Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Daher sieht die DSGVO für den Fall einer solchen Verletzung des Schutzes personenbezogener Daten folgende Melde- und Benachrichtigungspflich en vor:

Meldung an die zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt sowie Benachrichtigung der betroffenen Person, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, so muss er diese unverzüglich dem Verantwortlichen melden. Die Meldung einer Datenschutzverletzung an die Aufsichtsbehörde muss unverzüglich und möglichst binnen 72 Stunden, nachdem dem Verantwortlichen diese Verletzung bekannt wurde, erfolgen. Erfolgt die Meldung erst nach Ablauf von 72 Stunden, so ist diese Verzögerung zu begründen.

PRÄVENTION

Es lohnt sich auch für allgemeine Fragestellungen und Anliegen zum Thema **Prävention** von Cybercrime die angebotenen Informationen auf der Webseite der WKO (**www.it-safe.at**) oder des Bundeskriminalamtes **(www.bundeskriminalamt.at/306/start.aspx)** durchzusehen.

Das verfügbare Informationsangebot ist umfangreich gegeben, auch bei Stellen der Arbeiterkammer, **SaferInternet.at**, dem Internet Ombudsmann, mimikama, um nur ein paar Beispiele zu nennen.

Sowohl die Meldestelle des Bundeskriminalamtes als auch die WKO Cyber Security Hotline hält hierzu eine Linksammlung aktuell.

Als Service findet man am Ende der B oschüre eine Liste von Stellen und deren Erreichbarkeit.

ZEITGERECHTE VORBEUGENDE ABLAUFORGANISATORISCHE MASSNAHMEN

Bereiten Sie sich in Ihrem Unternehmen rechtzeitig auf mögliche und wahrscheinliche Straftaten im Bereich Cybercrime vor. Um für das Risikomanagement einen Überblick zu den wichtigsten Phänomenen und Deliktsfeldern zu gewinnen, lohnt sich auch ein Download des aktuellen, jährlich erscheinenden **Cybercrime-Reports** von der Webseite des Bundeskriminalamts. (**www.bundeskriminalamt.at/306/**)

Zu den wichtigsten Formen des Cybercrime gehören beispielsweise Computersabotagen, Phishing-Mails, Informationsdiebstahl, Identitätsdiebstahl, Abo-Fallen, Money Mules, Ransomware, Fake-Shops, etc.
Bedenken Sie, dass die vorgeschlagenen Maßnahmen auch anderen wichtigen Bestimmungen dienlich sind. Bei entsprechender Unternehmensgröße binden Sie deshalb Datenschutzbeauftragte, Rechtsabteilung, Compliance, Presse – und Öffentlichkeitsabteilung, sowie den Betriebsrat vor der Kommunikation an die Mitarbeiterinnen und Mitarbeiter in Ihre Planungen mit ein.

Solche Verfahrensweisen geben bei einem tatsächlichen Ereignis die notwendige Handlungssicherheit, dienen zur Schadensbegrenzung und binden alle betroffenen Interessensgruppen Ihres Unternehmens (Lieferanten, Kundinnen und Kunden, Polizei, etc.) mit ein.

Folgende Maßnahmen werden empfohlen:

- Gehen Sie zu wahrscheinlichen Sicherheits-Vorfällen für Ihre Sparte und Ihr Unternehmen alle Szenarien und Entscheidungen durch und legen Sie vorab die Prozessschritte fest.

- Identifizie en Sie zu den Prozessen die jeweiligen Verantwortungen der handelnden Personen und überlegen Sie die jeweiligen Reaktionen auf einen Schadensfall.

- Stellen Sie Listen zu erforderlichen Ansprechstellen bereit und denken Sie neben den internen Kontakten auch an externe Verständigungen.

- Wenn Sie nach einem Ereignis die benötigten Informationen für die Meldung erhoben haben (siehe „Erstbeurteilung eines Cybercrime Vorfalls“) informieren Sie die Strafverfolgungsbehörden.

- Legen Sie dazu im Vorfeld fest, welche routinemäßig vom System erfassten Protokolle bzw. Logdaten als Beweismittel zur Verfügung stehen könnten.

- Planen Sie zudem eine professionelle Öffentlichkeitsarbeit für den Fall eines Cyber-Sicherheitsvorfalls. Diese hilft, mögliche Reputationsschäden zu vermeiden bzw. zu begrenzen.

Versuchen Sie durch regelmäßige Übungen im Unternehmen einerseits die Maßnahmen zu proben und zu schulen, als auch Verbesserungspotenziale rechtzeitig zu erkennen.

QUICK CHECK LISTE - **CYBERCRIME ANZEIGE**

☑	Bewahren sie Ruhe und gehen sie strukturiert vor
☑	Vermeiden Sie Veränderungen am Gerät, die Beweise verändern oder vernichten
☑	Kommunizieren Sie auf einen Cybercrime-Vorfall grundsätzlich über ein anderes System oder Kommunikationsmittel als das bereits infizier e!
☑	Nutzen Sie vor der Anzeigeerstattung, falls erforderlich, das kostenlose Service für alle WKO-Mitglieder und holen Sie sich österreich-weit die telefonische Erste Hilfe bei der 24h-Cyber-Security-Hotline unter 0800 888 133.
☑	Bereiten Sie sich auf die Anzeige vor (gesicherte Beweismittel, Kopien zu forensischen Zwecken, Ereignisprotokoll, Tatzeiträume, Tatorte, Schäden)
☑	Sammeln Sie Informationen zu betroffenen Systemen, Nachweise, Protokollinformationen, widerrechtliche installierte Programme oder auf das System kopierte Dateien, Datei- oder Konfigu ationsänderungen, gelöschte Log-Einträge oder Logdateien, widerrechtlich deaktivierte Schutzmechanismen am System
☑	Erstellen Sie eine Sachverhaltsdarstellung
☑	Stellen Sie Personen- und Kontaktdaten zur Verfügung

QUICK CHECK LISTE – **PRÄVENTION**

☑	Erstellen Sie einen Ablaufplan/Notfallplan
☑	Bereiten Sie eine Notfalltelefonliste mit aktuellen Kontakten und Stellen vor (interne und externe Kontakte), die ihnen Hilfe geben können
☑	Legen Sie eine Liste von Ansprechpartnerinnen und Ansprechpartnern sowie Institutionen nach definier en Prioritäten fest, die zu informieren sind
☑	Interne Leitfäden und Handlungsanweisungen erstellen und aktuell halten
☑	Kurzversion von Verhaltensinformationen erstellen und aktuell halten
☑	Bereiten Sie gegebenenfalls interne Protokoll-vorlagen vor
☑	Kompetenzen vorab festlegen
☑	Bestimmen Sie vorab die Vertretung des Unternehmens nach außen bzw. der Geschäftsführung
☑	Arbeitszeitaufzeichnungen nach dem Arbeitszeitgesetzt (AZG) aktuell halten
☑	Schulen Sie die Verantwortlichen und ihre Mitarbeiterinnen und Mitarbeiter
☑	Üben Sie den Ablauf im Rahmen von jährlichen Übungen
☑	Halten Sie Uhrzeit und die richtige Zeitzone auf allen Systemen aktuell

☑	Halten Sie ihre Systeme und Software aktuell und spielen sie erforderliche Sicherheitsupdates ein
☑	Machen Sie regelmäßig Backups
☑	Technische Planung auf modulare Systeme, getrennte Datenspeicherung, segmentierte Netze prüfen und ggf. berücksichtigen
☑	Cloud-Anbieter sollten die Mehrfach-Mandantenumgebung sauber getrennt halten inkl. entsprechender Logdateien mit rechtskonformer Aufbewahrungszeit
☑	Weisen Sie Cloud-Anbieter insbesondere auch auf Manipulationsschutz und Nachvollziehbarkeit von Handlungen oder Konfigu ationen (extern/intern) hin
☑	Festlegung im Vorfeld, welche routinemäßig vom System erfasste Protokolle bzw. Logdaten als Beweismittel zur Verfügung stehen könnten
☑	Legen sie die Kommunikationskanäle fest
☑	Planung einer professionellen Öffentlichkeitsarbeit für den Fall eines Cyber-Sicherheitsvorfalls (Thema Reputationsschäden vermeiden bzw. begrenzen)

WEITERE INFORMATIONEN UND HILFE

Bundeskriminalamt Meldestelle Cybercrime
Kontakt: against-cybercrime@bmi.gv.at
Beweismittel upload: https://cryptshare.bmi.gv.at

WKO CYBER-SECURITY-HOTLINE 0800 888 133
Kostenloses Service für alle WKO-Mitglieder
Rasche Hilfe bei Cyber-Attacken! www.cys.at

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
Telefon: 01 531260

WKO Experts Group IT Security
https://www.itsecurityexperts.at
offi e@itsecurityexperts.at

WKO InternetTV
https://www.cysec.tv

Sicherheitshandbuch IT SAFE
Unternehmen:
Mitarbeiter:

Rechtsinformationssystem der Republik Österreich
https://www.ris.bka.gv.at/

Österreichisches Informationssicherheitshandbuch
https://www.sicherheitshandbuch.gv.at/

Österreichische Datenschutzbehörde
Barichgasse 40-42, 1030 Wien
Telefon: +43 1 52 152-0
E-Mail: dsb@dsb.gv.at

Bundesministerium für Justiz
Museumstraße 7, 1070 Wien
Telefon: 0800 99 99 99

Verein Mimikama®
https://www.mimikama.at/

Internet Ombudsmann
https://www.ombudsmann.at/

Initiative Safer Internet
https://www.saferinternet.at

Arbeiterkammer Wien
Prinz Eugen-Straße 20-22, 1040 Wien
Telefon: 01 501650
https://wien.arbeiterkammer.at

GLOSSAR

Abofalle : Abofalle bezeichnet umgangssprachlich eine weit verbreitete unseriöse Geschäftspraktik im Internet, bei der Verbraucher unbeabsichtigt ein kostenpflichtiges Abonnement eingehen

AZG : Arbeitszeitgesetz

Backup : Datensicherung eines Systems oder Datenträgers das zur Wiederherstellung im Fehlerfall genutzt werden kann (Sicherungskopie)

BK : Bundeskriminalamt

C4 : Cyber Crime Competence Center, ist die nationale und internationale Koordinierungs- und Meldestelle für Ermittlungen im Zusammenhang mit Cybercrime und für die elektronische Beweismittelsicherung und deren Auswertung im Bundeskriminalamt zuständig

Cloud : Internetbasierte Bereitstellung von Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung

Cryptshare : Die Cryptshare® Web-Anwendung ermöglicht den einfachen und sicheren Austausch vertraulicher Informationen durch die verschlüsselte Ablage von Dateien und Nachrichten auf dem Cryptshare-Server des Innenministeriums.

DSGVO : Datenschutzgrundverordnung zum Schutz personenbezogener Daten, die EU Verordnung wurde im Mai 2018 europaweit eingeführt.

Forensik : Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen kriminelle Handlungen systematisch untersucht werden. Der Begriff stammt vom lateinischen „forensis"

Image : Ist die idente Kopie eines Systems bzw. Datenspeichers.

Money Mules : Personen, die im Internet rekrutiert werden und sich durch die Weiterleitung illegaler Gelder der Geldwäscherei strafbar machen.

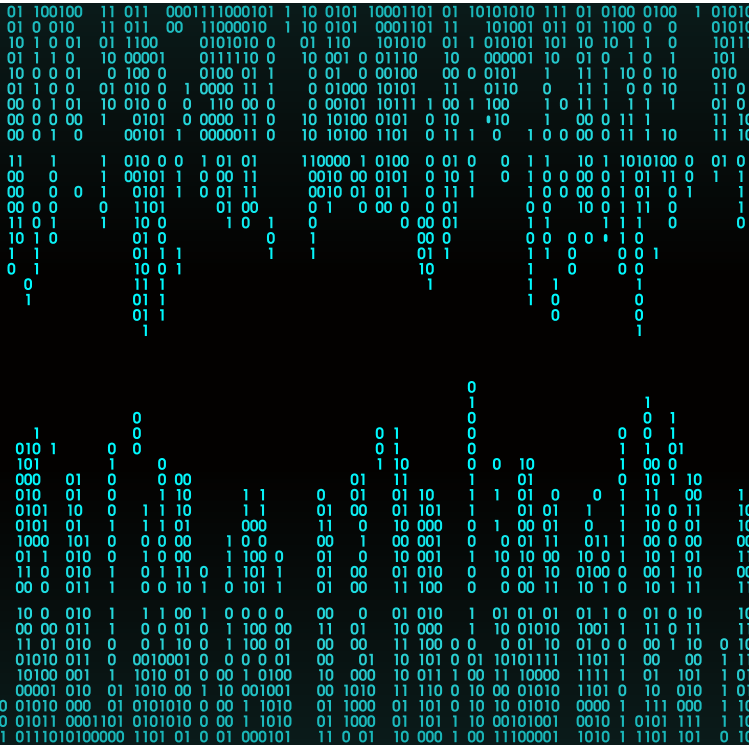
Ransomware : Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann.

Social Engineering : Bei Social Engineering handelt es sich um ein Verfahren, um sicherheitstechnisch relevante Daten durch das Ausnutzen menschlichen Verhaltens zu gewinnen. Dabei wählt der Täter den Menschen als vermeintlich schwächtes Glied der Sicherheitskette aus, um seine kriminellen Absichten in die Tat umzusetzen.

SOKO CLAVIS : Sonderkommission (SOKO) im Bundeskriminalamt, die aufgrund des Anstieges der Erpressungen durch Ransomware in Österreich Anfang Juni 2016 im C4 eingerichtet wurde.

NOTIZEN

NOTIZEN



Bundesministerium
Inneres

Bundeskriminalamt

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

GEMEINSAM.SICHER
in Österreich

EXPERTS GROUP IT-SECURITY