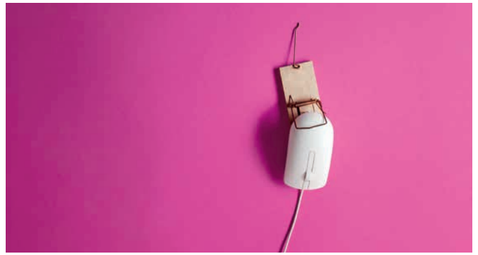
POLICE

Cyberangriff – was nun?
Empfehlungen für Betroffene

Wenn Sie von einem Cyberangriff betroffen sind oder einen solchen vermuten, ist rasches Handeln entscheidend. Folgende Empfehlungen helfen Ihnen, Angriffe zu bewältigen, Schaden zu begrenzen und Bekannte in Ihrem Umfeld zu schützen.

Ergreifen Sie Sofortmassnahmen

> Vermuten Sie eine Infektion mit einer Schadsoftware? Trennen Sie betroffene Geräte vom Internet. Lassen Sie sich von einer Fachperson beraten.
> Haben Sie Passwörter weitergegeben? Ändern Sie diese sofort.
> Haben Sie Kreditkarten- oder Bankinformationen weitergegeben oder eine Zahlung getätigt? Sperren Sie die Karte und informieren Sie umgehend Ihre Bank.
> Sind Ihre amtlichen Dokumente in kriminelle Hände geraten? Lassen Sie die Dokumente bei der kantonalen Passstelle oder der Polizei annullieren.
> Warnen Sie Bekannte vor kriminellen Aktivitäten, die in Ihrem Namen getätigt werden.



Melden Sie den Vorfall

Bei Schaden: Anzeige bei der Polizei
Bei Straftaten, beispielsweise Hacking, Betrug oder Erpressung, melden Sie sich umgehend bei der Polizei. Dies insbesondere dann, wenn sie Zahlungen getätigt haben oder den Verlust persönlicher Daten feststellen.

> Wählen Sie in dringenden Fällen die Notrufnummer 112
> Erstatten Sie Anzeige. Vereinbaren Sie dazu einen Termin auf einer Polizeiwache.
> Halten Sie Beweismittel bereit. Dazu gehören Nachrichten und Kontaktangaben der Täterschaft, Banknachweise und betroffene Geräte.
> Setzen Sie Geräte möglichst erst nach der Spurensicherung durch die Polizei neu auf.

Nach der Anzeigeerstattung und der Beweisaufnahme nimmt die Polizei weiterführende Ermittlungen auf. Ziel ist es, einen allfälligen Zusammenhang mit anderen Fällen zu prüfen sowie die Täterschaft zu überführen. Das Verfahren führt die zuständige Staatsanwaltschaft.

Ohne Schaden: Meldung an das Nationale Zentrum für Cybersicherheit
Jede Meldung hilft dabei, kriminelle Tätigkeiten frühzeitig zu erkennen und darauf zu reagieren. Melden Sie auch erfolglose Cyberangriffe oder Betrugsversuche ohne Schaden beim Nationalen Zentrum für Cybersicherheit:

Nationales Zentrum für Cybersicherheit,
www.report.ncsc.admin.ch

Nehmen Sie sich vor Folgeangriffen in Acht

Bleiben Sie auch nach einem Cyberangriff wachsam. Kriminelle können mit den bereits gesammelten Informationen einen weiteren Betrugsversuch starten oder sich erneut Zugang zu Ihrem Gerät verschaffen.

Kantonspolizei Bern
Waisenhausplatz 32
3011 Bern

police.be.ch/cyber

POLICE

Sicher unterwegs – auch im Internet

Empfehlungen für Privatpersonen

Um sich gegen Cyberangriffe zu schützen, braucht es eine Kombination von technischen Massnahmen und richtigem Verhalten. Folgende Empfehlungen helfen Ihnen, Ihre Sicherheit in der digitalen Welt zu erhöhen.

Lassen Sie sich nicht hinters Licht führen

Kriminelle verschleiern Ihre Identität, indem sie sich als vertrauenswürdige Personen ausgeben. Erschweren Sie Kriminellen das Handwerk:

> Geben Sie keine vertraulichen Informationen oder Daten weiter. Dazu gehören Passwörter, Gutscheincodes, Kreditkarteninformationen, amtliche Dokumente sowie intime Fotos.
> Übergeben Sie kein Geld oder Wertsachen an Personen, die Sie nicht persönlich kennen.
> Gewähren Sie niemandem Zugriff auf Ihr E-Banking oder auf Ihren Computer.
> Seien Sie skeptisch gegenüber grossen Gewinnversprechen oder verlockenden Schnäppchen.
> Seien Sie misstrauisch, wenn die «grosse Liebe» oder angebliche Bekannte im Netz Sie um finanzielle Unterstützung bitten.
> Seien Sie sparsam beim Veröffentlichen von persönlichen Informationen auf Webseiten, in sozialen Netzwerken oder Chats. Kriminelle sammeln diese, um Attacken vorzubereiten.
> Klicken Sie nicht auf verdächtige Links. Laden Sie keine Dateien oder Programme herunter, die Ihnen merkwürdig erscheinen.

Schützen Sie Ihre Systeme und Daten

Kriminelle machen sich technische Schwachstellen zu Nutze, um in Systeme einzudringen und auf Daten zuzugreifen. Erschweren Sie Kriminellen den Zugriff:

> Verwenden Sie sichere Passwörter. Ein gutes Passwort:
  > ist zufällig generiert und besteht aus mindestens zwölf Zeichen.
  > enthält Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.
  > wird nur jeweils nur für eine einzige Anwendung verwendet. Ein Passwortmanager hilft Ihnen, die verschiedenen Passwörter zu verwalten.
  > wird mit einer Zwei-Faktor-Authentifizierung ergänzt.
> Verwenden Sie Geräte mit integrierten Sicherheitsfunktionen. Aktivieren Sie Firewall, Viren- und Bedrohungsschutz, automatische Updates und Webfilter.
> Deaktivieren Sie Makros in Office-Anwendungen. Diese sind potenzielle Einfallstore für Schadsoftware.
> Trennen Sie Ihren Internetzugang in ein Hauptnetzwerk und ein Gastnetzwerk für Drittpersonen und smarte Haushaltsgeräte.
> Sichern Sie regelmässig Ihre Daten. Erstellen Sie Backups einmal offline, beispielsweise auf einer externen Festplatte, und einmal online in einer Cloud.

Bleiben Sie informiert

Cyberkriminelle sind kreativ und entwickeln laufend neue Strategien und Vorgehensweisen. Lernen Sie die aktuellen kriminellen Handlungen im Internet und entsprechende Schutzmassnahmen kennen:

Kantonspolizei Bern
www.police.be.ch/cyber

Nationales Zentrum für Cybersicherheit,
www.ncsc.admin.ch

Cybercrimepolice,
www.cybercrimepolice.ch

iBarry – Plattform für Internetsicherheit,
www.ibarry.ch

Card Security – Kartensicherheit beim Online-Shopping, www.card-security.ch

Schweizerische Kriminalprävention,
www.skppsc.ch

Kantonspolizei Bern
Waisenhausplatz 32
3011 Bern

police.be.ch/cyber