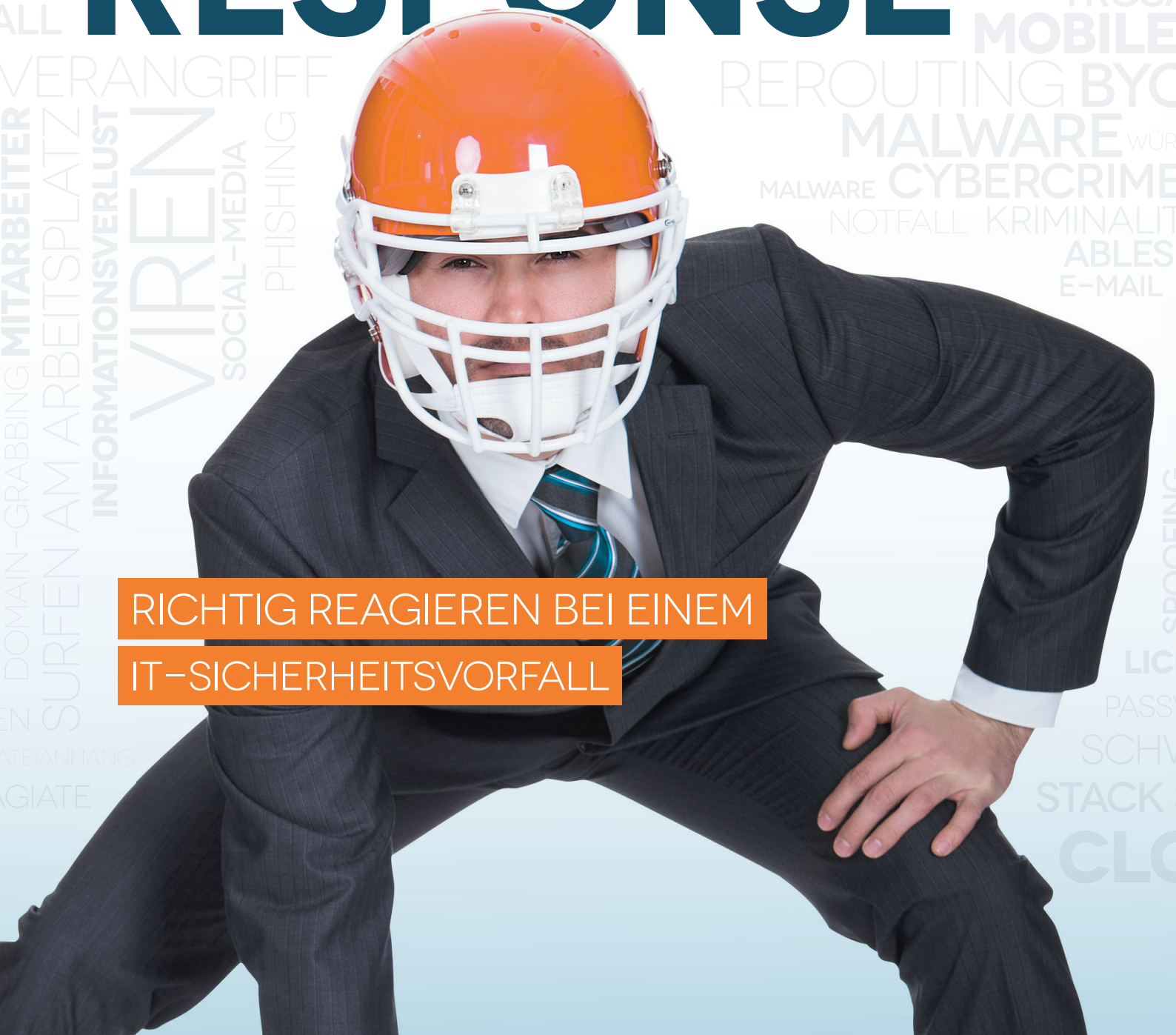
IHK NRW - Die Industrie- und Handelskammern in Nordrhein-Westfalen

INCIDENT RESPONSE



RICHTIG REAGIEREN BEI EINEM IT-SICHERHEITSVORFALL

EINLEITUNG

Die Führung eines Unternehmens ist für dessen reibungslosen Ablauf verantwortlich. IT-Systeme spielen dabei in den meisten Organisationen eine wichtige, in manchen sogar eine zentrale Rolle. Im digitalen Zeitalter kann ein Ausfall dieser Systeme zum völligen Stillstand und im schlimmsten Fall sogar zur Insolvenz des Unternehmens oder zumindest zu hohen Schadensersatzforderungen führen. Auch drohen Imageschäden und der Verlust von Zertifizierungen. Daraus resultieren möglicherweise Kundenverlust sowie Gesetzesverstöße mit kaum vorhersehbaren Folgen. Daher ist das richtige Vorgehen bei einem IT-Sicherheitsvorfall von entscheidender Bedeutung.

ZIEL DIESES LEITFADENS

Ziel dieses Leitfadens ist, Ihnen zu helfen, bei einem IT-Sicherheitsvorfall „richtig" vorzugehen (Incident Response). Vorsorge ist die beste Medizin, jede Organisation ist individuell und benötigt daher individuell angepasste Maßnahmen. Das Thema ist komplex. Dieser Leitfaden kann und soll daher keine abschließende Betrachtung des Themas sein und auch nicht in die fachliche Tiefe gehen. Er soll Ihnen als Entscheider oder Anwender in einer Organisation die wichtigsten „Merkpunkte" und geeignete Ansprechpartner für die Praxis mit auf den Weg geben. Tiefergehende Informationen bietet z.B. das Bundesamt für Sicherheit in der Informationstechnik in Form der IT-Grundschutz-Kataloge (Abschnitt „B 1.8 Behandlung von Sicherheitsvorfällen", https://www.bsi.bund.de/DE/Themen/ITGrundschutz/grundschutz.html)

WIE ERKENNE ICH EINEN IT-SICHERHEITSVORFALL?

Kurz gesagt: Nicht jedes auffällige Ereignis ist auch ein Sicherheitsvorfall. Ernst wird die Lage aber meist dann, wenn

- die **Vertraulichkeit** Ihrer Daten nicht mehr gewährleistet ist (Jemand hat ihre Daten „geklaut", oder Sie haben aus Versehen eine wichtige E-Mail an einen falschen Empfänger versendet.)
- die **Verfügbarkeit** betroffen ist (Ihr wichtiger E-Commerce-Server ist plötzlich nicht mehr erreichbar, oder eine Festplatte mit kritischen Daten ist defekt.)
- die **Integrität** nicht mehr gewährleistet ist (Plötzlich stimmt Ihre Buchhaltung nicht mehr, oder einer Ihrer Computer ist von einem Trojaner befallen.)

Sie sollten daher besonders in Bezug auf Ihre wichtigen IT-Systeme und Daten aufmerksam sein und auch Ihr Team motivieren, mit Auffälligkeiten offen umzugehen. Im Zweifel helfen Ihnen Ihr IT-Administrator oder andere IT-Experten bei einer Ersteinschätzung der Lage. Wichtig ist: schnell und angemessen reagieren.

TYPISCHE FRAGEN BEI EINEM IT-SICHERHEITSVORFALL

Besonders in kleineren Unternehmen tauchen oft ähnliche Fragen auf: Wen rufe ich „im Ernstfall" am besten an? Wie merke ich, dass ich angegriffen werde oder wurde? Wie kann ich meine IT-Dienstleister am schnellsten erreichen? Wie soll ich vorgehen und was in welcher Reihenfolge durchführen? Wem kann ich dabei trauen und wem nicht? Bei wem bekomme ich Rat? Und nicht selten am drängendsten: Welcher Schaden ist entstanden oder kann noch entstehen, wie kann ich weiteren Schaden vermeiden und wie teuer wird es für mich? Optimal ist es, wenn Sie diese Fragen vor einem möglichen Vorfall einmal „im Geiste" durchspielen. Wie gut sind Sie vorbereitet?

HÄUFIGE FEHLER BEI EINEM IT-SICHERHEITSVORFALL

Handlungsanweisungen und Dokumentationen erfolgen zu unpräzise

„Bitte sichern Sie vorab unsere Protokolldateien, damit die externen Experten diese untersuchen können, wenn sie bei uns sind" ➜ Dritte kennen Ihren Bedarf und Ihre Situation nicht immer passgenau. Welche Protokolldateien sind gemeint? Die vom „gehackten" Web-Server oder zusätzlich die Ihres E-Mail-Servers? Wann genau ist etwas passiert?

Beweise/Daten werden vorschnell vernichtet

„Als Ihr IT-Dienstleister machen wir jetzt folgendes: Wir lassen über alle Rechner einen Virenscanner laufen und löschen alle Funde. Danach ist Ihr System wieder sauber." ➜ Schnell wieder einsatzfähig sein ist wichtig, aber erstellen Sie eine Quarantäne-Kopie von digitalen Schädlingen, damit im Ernstfall IT-Experten genau untersuchen können, was passiert ist.

Es geht zu viel Zeit verloren

„Ihr Sicherheitsvorfall liegt nun 4 Wochen zurück. Leider rufen Sie uns erst jetzt. Die Spuren X, Y und Z sind nun definitiv nicht mehr verfügbar." ➜ Auch in der digitalen Welt ist unverzügliches Reagieren oft unerlässlich, denn „digitale Fingerabdrücke" verwischen oft sehr schnell.

Generell zu wenig Zeit/Ressourcen

„Wie, Sie können den Täter nicht innerhalb von zwei Tagen finden? Aber Sie sind doch IT-Experte! Dann lasse ich den Fall lieber doch nicht untersuchen" ➜ Je komplexer Ihre IT-Infrastruktur und je umfangreicher Ihre Datenbestände, desto aufwändiger die notwendigen Untersuchungen.

Nicht ausreichend im Team gearbeitet

„So, die Experten sollen jetzt mal ihre Arbeit machen, damit ich mich wieder voll auf mein Geschäft konzentrieren kann" ➜ Gute IT-Experten können Sie entlasten, aber für wichtige Rückfragen und Entscheidungen sollten Sie stets erreichbar sein.

Komplexität der Zielsysteme unterschätzt

„Herr Geschäftsführer, Sie hatten uns von Bring Your Own Device und Ihren vielen Auslandsstandorten überhaupt nicht berichtet" ➜ Ihr IT-Experte benötigt im Ernstfall vollständige, aktuelle und umfassende Informationen, um Sie bestmöglich unterstützen zu können.

Juristische Aspekte bleiben unberücksichtigt

„Der Täter ist bestimmt unser ungeliebter Kollege Herr Superböse. Untersuchen Sie seinen PC und schauen Sie auch einmal, ob er E-Mails mit unseren Daten an die Konkurrenz versendet hat" ➜ Gesetzliche Rahmenbedingungen wie das Bundesdatenschutzgesetz, die EU-Grundschutzverordnung oder die Einbindung des Betriebsrates müssen bei jedem Schritt berücksichtigt werden.

DEFINITION

IT-SICHERHEITSVORFALL (INCIDENT)

Ereignis analog einem Notfall, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen, für welche Sie einen hohen oder sehr hohen Schutzbedarf definiert haben, in Ihrem Unternehmen / Ihrer Organisation derart beeinträchtigt, dass ein großer Schaden für Ihr Unternehmen / Ihre Organisation / Ihre Kunden oder Geschäftspartner entstehen kann.

RICHTIG REAGIEREN BEI EINEM IT-SICHERHEITSVORFALL

Bewahren Sie Ruhe und lassen Sie den Ernst der Lage prüfen. Egal ob ein „unachtsamer Klick“ oder ein fortgeschrittener IT-Angriff - nur mit Ihrer rechtzeitigen Unterstützung und Mitarbeit können interne oder externe Experten den Fall aufklären und lösen.

Die nachfolgende Liste soll Ihnen helfen, bei einem möglichen IT-Sicherheitsvorfall bestmöglich zu handeln. Wir empfehlen Ihnen daher, diese Liste sofort greifbar aufzubewahren.

1. Reagieren Sie überlegt aber zügig. Erzeugen Sie möglichst keine Aufregung im Unternehmen. Weder auf die lange Bank schieben noch Panik sind gute Lösungen.
2. Prüfen Sie welche Personen vertrauenswürdig oder voreingenommen sind bzw. möglicherweise im Fokus stehen. Holen Sie dann Expertenrat ein. Qualifizierte Fachexperten sollten rechtzeitig eingebunden werden. Bilden Sie gegebenenfalls ein Krisenreaktionsteam. Sorgen Sie für eine verlässliche Unterstützung durch Ihren externen Dienstleister.
3. Priorisieren Sie Ihr weiteres Vorgehen und weihen Sie nur erforderliche und vertrauenswürdige Personen ein.
4. Stellen Sie wenn möglich betroffene Geräte, Daten und Backups sicher. Prüfen Sie, ob alle wichtigen Daten in einem funktionsfähigen Backup vorhanden sind. Achten Sie auf die Vollständigkeit, Aktualität und Integrität der Daten. Lassen sich gesicherte Daten wirklich öffnen und zurückspielen?
5. Wenn das Smartphone oder ein anderes Mobilgerät abhandengekommen ist, prüfen Sie, ob verbundene Dienste oder Accounts abrufbar sind und sperren Sie diese bei Bedarf.
6. Verändern Sie die Daten nicht, um keine Spuren zu verwischen. Arbeiten Sie stattdessen mit geeigneten (forensischen) Kopien.
7. Dokumentieren Sie den Vorfall sorgfältig. Protokollieren Sie dazu durchgeführte Schritte und Ihre Beobachtungen umfangreich und genau, z.B. durch Fotos und exakte Zeitangaben.

   Beispiel: Am 01.04. um ca. 14:30 Uhr habe ich eine E-Mail mit einem angehängten Lieferschein erhalten. Die ZIP-Datei habe ich geöffnet, aber nicht gespeichert. Es öffnete sich kurz ein schwarzes Fenster. Ansonsten ist nichts passiert. Am darauf folgenden Tag konnte ich keine Word-Dateien mehr öffnen. Auf meinem Bildschirm erschien eine Warnung des FBI bezüglich illegaler Aktivitäten mit einer Zahlungsaufforderung zwecks Strafe. Anbei befindet sich ein Foto von der Warnung, das ich mit meinem Handy erstellt habe.
8. Entwickeln Sie unterschiedliche Szenarien:
   - Wie reagiert man auf einen Innentäter?
   - Wie reagiert man darauf, wenn Kundendaten in fremde Hände geraten sind?
   - Wie lassen sich verlorene Daten wiederherstellen?
   - Was ist, wenn die eigenen IT-Systeme nicht mehr vertrauenswürdig sind?

„Better safe than sorry – Ein Fehlalarm ist besser als ein übersehener Sicherheitsvorfall.“

EINFACHE PRÄVENTIVE MASSNAHMEN

Am besten sind Sie gut vorbereitet! Dazu hilft ein aktueller und vollständiger Infrastrukturplan (Was steht wo, Netzwerkplan, Konfiguration), ein Incident Response Plan (Liste zum „Abarbeiten“ für den Ernstfall) und die präventive Kontaktaufnahme mit Ihren IT-Dienstleistern. Erarbeiten Sie mit diesen gemeinsam einen (kleinen) Plan, der die wichtigsten Punkte und Maßnahmen kurz skizziert.

IHK NRW - Die Industrie- und Handelskammern in Nordrhein-Westfalen e. V.
Berliner Allee 12
40212 Düsseldorf
Tel.: 02 11 / 3 67 02 - 0
Fax: 02 11 / 3 67 02 - 21
E-Mail: info@ihk-nrw.de
Internet: www.ihk-nrw.de

Sicherheitspartner Nordrhein-Westfalen gegen Wirtschaftsspionage und Wirtschaftskriminalität

GEEIGNETE ANSPRECHPARTNER

Um erfolgreich auf einen IT-Sicherheitsvorfall reagieren zu können, bedarf es interdisziplinärer Kompetenzen. Haben Sie dazu schon an die nachfolgenden Ansprechpartner gedacht?

Eigene Kräfte - das Steuer in der Hand behalten
IT-Sicherheitsbeauftragter (wenn in Ihrem Unternehmen organisiert), Datenschutzbeauftragter (wenn in Ihrem Unternehmen bestellt), das eigene IT-Team

Externer IT-Sachverstand, neutral und objektiv:
Anlaufstelle für öffentlich bestellte und vereidigte Sachverständige sind Ihre örtliche IHK und das Online-Verzeichnis https://svv.ihk.de mit Suche nach Fachgebiet „Informationssysteme“

Technische Betreuung, insbesondere operational:
IT-Dienstleister, IT-Systemhäuser

Rechtliche Fragen, z.B. Arbeitsrecht, Strafrecht:
Rechtsanwälte

Krisenreaktion:
PR-Berater

Aufklärung von Straftaten und behördliche Beratung:
Bundeskriminalamt, Landeskriminalämter sowie lokale Polizei, Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik

INHALT

Martin Wundram, Sachverständiger Informationstechnologie insbesondere IT-Sicherheit und IT-Forensik, DigiTrace GmbH, Zollstockgürtel 59, 50969 Köln

ANSPRECHPARTNER IT-SICHERHEITSTAG NRW

IHK Köln
Dieter Schiefer
Telefon: +49 221 1640-520
Email: dieter.schiefer@koeln.ihk.de

Unterstützt durch
DigiTrace
Kompetenz in IT-Forensik
www.digitrace.de