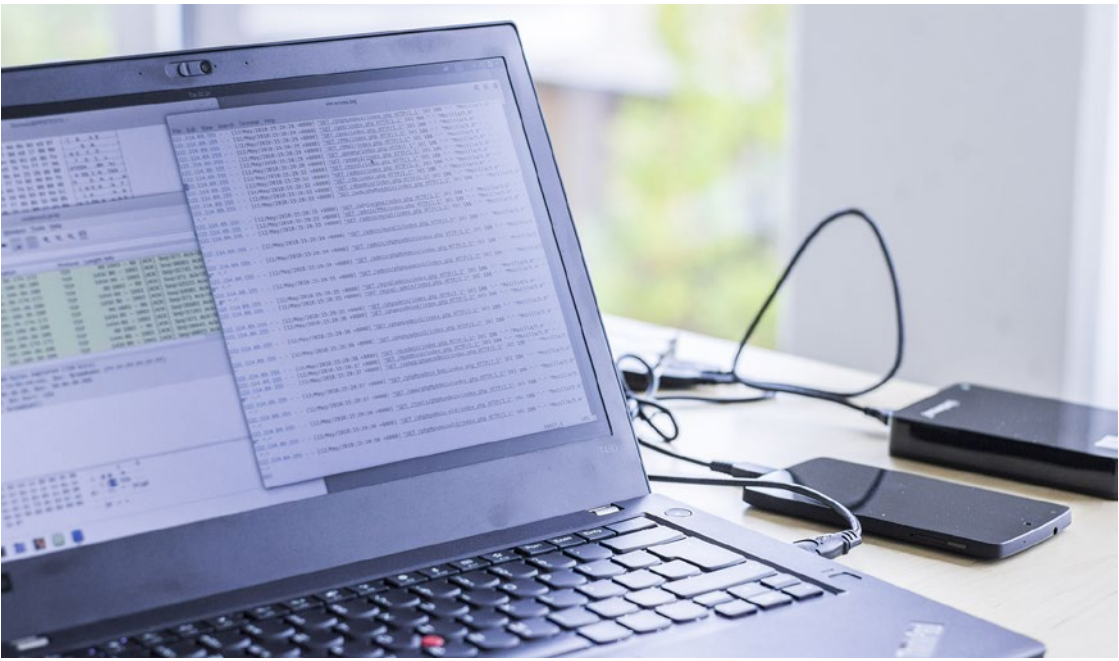


IT-Forensik und Incident Response

Aufklärung von IT-Sicherheitsvorfällen

datenschutz nord GRUPPE

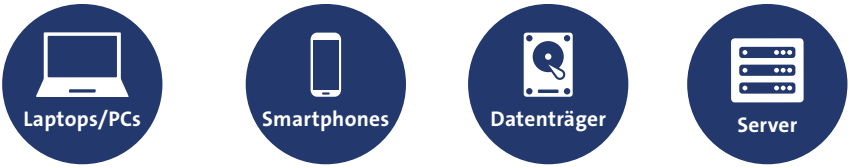
Aufklärung von IT-Sicherheitsvorfällen

Zur Klärung eines **IT-Sicherheitsvorfalls** ist die **IT-Forensik** das Mittel der Wahl. Die Methoden der digitalen Forensik ermöglichen im Falle eines kompromittierten Systems eine Rekonstruktion des **Angriffs** und eine Abschätzung der möglichen Auswirkungen. Die Ergebnisse der forensischen Untersuchung unterstützen zudem eine Planung der weiteren Vorgehensweise zur **Schadensreduktion** und zu zukünftigen **Sicherungsmaßnahmen.** Sofern bei einem Angriff **Schadsoftware** hinterlegt wurde, kann durch eine forensische Analyse festgestellt werden, welche Funktion die Schadsoftware hat (z.B. Kopieren von Unternehmensdaten oder das Etablieren eines langfristigen Zugriffs) und ob ggf. weitere Systeme im Netzwerk infiziert wurden.

Wenn der Verdacht besteht, dass ein Mitarbeiter Daten aus dem Unternehmen weitergibt oder **Sabotage** durchführt, ist eine schnelle Klärung des Falles wichtig, um Schaden vom Unternehmen abzuwenden. Eine forensische Untersuchung der betroffenen Systeme und ggf. des Netzwerkverkehrs kann hier wertvolle und falls nötig **gerichtsverwertbare Ergebnisse** erzielen.

Bei der Verletzung des Schutzes **personenbezogener Daten** ist gemäß Artikel 33 DSGVO der Verantwortliche verpflichtet, den Vorfall binnen 72 Stunden der zuständigen Aufsichtsbehörde zu melden. Eine zeitnah durchgeführte forensische Untersuchung kann Aufschluss darüber geben, ob überhaupt personenbezogene Daten betroffen waren (und daher **keine Meldepflicht** besteht), welcher Art die Daten waren und welches Ausmaß der Vorfall hat. Auch hier liefert die IT-Forensik wichtige Ergebnisse zum weiteren Vorgehen und zur Ausgestaltung der Sicherungsmaßnahmen.

Typische **Untersuchungsgegenstände** sind:



Unsere Vorgehensweise

1 Vorbesprechung

Zu einer korrekten **forensischen Analyse** gehört eine ausgiebige **Vor- und Nachbereitung.** Zu Beginn werden in einer (ggf. telefonischen) Vorbesprechung der Verdacht oder der Vorfall erläutert, sowie die Ziele der durchzuführenden Untersuchungen diskutiert. Im Rahmen der Vorbereitung werden gegenseitige Ansprechpartner für das Analyseprojekt festgelegt.

2 Spurensicherung

Anschließend werden vor Ort oder per Fernzugriff **Daten und mögliche Spuren** gesichert. Die Durchführung der Sicherung hängt vom zu untersuchenden System ab. Beispielsweise können **Datenträgerabbilder** (Images) oder einzelne Dateien per Fernzugriff übertragen werden. Falls ein Livesystem (z.B. ein eingeschaltetes Notebook) zu untersuchen ist, muss die **Spurensicherung vor Ort** am bis dahin in Betrieb befindlichen System durchgeführt werden.

3 Analyse

Zur **Sicherstellung der Integrität** des Untersuchungsgegenstands, und damit der Wahrung einer gerichtsverwertbaren, digitalen Beweiskette, werden bei Datenträgerabbildern und Dateien **Hashverfahren** zur Berechnung von Prüfsummen eingesetzt. Auf den Datenträgerabbildern werden die für den Fall relevanten Daten extrahiert und auf **Auffälligkeiten und Zusammenhänge** analysiert. Die einzelnen Analyseschritte werden schriftlich und je nach Bedarf auch fotografisch protokolliert und dokumentiert.

4 Dokumentation

Bereits während der Analyse-Phase können dem Auftraggeber relevante Informationen und **Handlungsempfehlungen** mitgeteilt werden, um frühzeitig zur **Behebung bzw. Aufklärung** des Vorfalls beizutragen. Nach der Analyse werden die Ergebnisse ausführlich und nachvollziehbar dokumentiert und ggf. Handlungsempfehlungen gegeben.

So können wir Sie unterstützen

Feststellung und Untersuchung von Server-Angriffen (Incident Response)

Ein Großteil der erfolgreichen Server-Angriffe findet auf **Webseiten** statt. Die Folge eines solchen Angriffs kann der **Diebstahl von sensiblen Daten,** wie beispielsweise **Zahlungsdaten** von Kunden oder **Abrechnungsdaten** sein. Zudem lassen sich kompromittierte Webseiten und -server zum Versenden von **Spam-Mails,** zur Verbreitung von **Schadsoftware** oder zum Bereitstellen von **Phishing-Seiten** nutzen. Ein derartiger Angriff kann somit auch den Ruf des Betreibers schädigen.

In einem solchen Fall führen wir zunächst eine Identifikation der auf dem Server installierten Dienste durch. Daraufhin werden die Serverdaten von uns gesichert und detailliert analysiert, um den **Angriffsvektor** bzw. die ausgenutzte **Schwachstelle** zu identifizieren. Ist die Schwachstelle identifiziert, können Sie auf Basis unserer Empfehlungen schnell **Maßnahmen zur Behebung** umsetzen. Weiterführend werden von uns das Ausmaß des Angriffs, sowie die Art und der Umfang der betroffenen Daten festgestellt. Dies ermöglicht es Ihnen, eine zielgerichtete Benachrichtigung der betroffenen Nutzer und eine umfängliche **Bereinigung und Wiederherstellung** des betroffenen Systems durchzuführen und zukünftige Sicherungsmaßnahmen zu planen.

Feststellung und Identifizierung von installierter Schadsoftware und Analyse der durchgeführten Aktionen

Besteht bei Ihnen der Verdacht einer **Infektion** eines Systems (z.B. Laptop oder Arbeitsplatz-PC) mit **unbekannter Schadsoftware,** können wir Ihnen helfen, die Funktionsweise der Schadsoftware zu verstehen, um die **Auswirkungen** auf das Unternehmen besser bewerten zu können und **Gegenmaßnahmen** umzusetzen.

Durch eine genaue Untersuchung des **kompromittierten Systems** können wir unter anderem von der Schadsoftware veränderte oder gelöschte Dateien identifizieren und ggf. wiederherstellen. Weiterhin untersuchen wir die möglichen **Infektionswege** und identifizieren und analysieren die von der Schadsoftware geöffneten Internetverbindungen, um Erkenntnisse über **ausgespähte Informationen** und weitere kompromittierte Systeme in Ihrem Netzwerk zu erlangen.

Untersuchung von Smartphone/Tablets

Ein ungewöhnlich hoher **Daten- und Stromverbrauch** von mobilen Geräten kann auf die Installation einer **Schad-App** oder eine anderweitige Kompromittierung hindeuten.

Durch Analyse des Geräts können wir die Herkunft bzw. den Installationsweg der Schad-App identifizieren. Ist eine solche App gefunden worden, wird von uns die Funktionsweise der App analysiert, um eventuelle weitere von der App durchgeführte Aktionen zu ermitteln.

Untersuchung eines Datenlecks (Data Breach)

Bei einer **Verletzung des Schutzes personenbezogener Daten** können wir helfen, die **Art und den Umfang** der betroffenen Daten festzustellen. Auch bei der Klärung der **Ursache** des Vorfalls können wir Sie unterstützen

In einem solchen Fall können sowohl Server, Laptops/PCs als auch Smartphones und mobile Datenträger wie z.B. USB-Sticks Untersuchungsgegenstände sein.

Wiederherstellung von gelöschten Dateien (Datenrettung)

Wurden Daten versehentlich **gelöscht,** oder sind während eines Schadsoftwarebefalls verloren gegangen, können mit Hilfe spezieller Programme **Wiederherstellungsversuche** der betroffenen Dateien vorgenommen werden. Dazu wird in der Regel eine **1:1-Kopie** des entsprechenden Datenträgers oder ein entsprechendes **Abbild** benötigt. Im Anschluss an eine erfolgreiche Wiederherstellung werden die Daten auf einem Datenträger zur Verfügung gestellt.

Untersuchung von Dateizugriffen bzw. -änderungen

Ein weiterer Anwendungsfall ist die Untersuchung von ungewöhnlichen Dateizugriffen bzw. -änderungen. Hierbei werden von uns in der Regel **Metainformationen** des Dateisystems oder Protokolldaten des Betriebssystems genutzt, um die Ursache zu ermitteln.

Sofern Sie keinen definierten Incident-Prozess haben, können Sie bei einem Vorfall die folgenden **Erste-Hilfe-Schritte** durchführen. Sollten Sie sich dabei unsicher sein, könne Sie uns gerne kontaktieren.

Erste Schritte im Notfall

Ruhe bewahren!

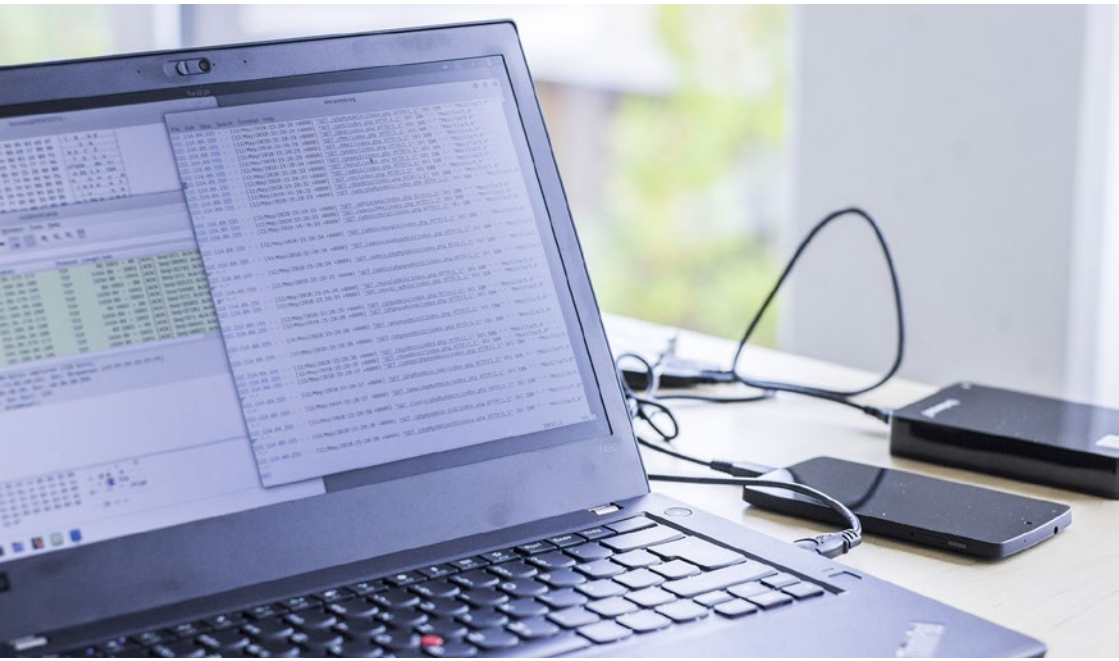
Im Falle von **Ransomware/Erpressungstrojanern: Trennen** Sie das betroffene System vom **Strom,** um eine weitere Verschlüsselung von Daten und Verbreitung zu verhindern.

Versuchen Sie **keine Änderungen am System** vorzunehmen, um keine Spuren zu vernichten.

Fertigen Sie ein **Gedächtnisprotokoll** des Vorfalls an.
Was ist passiert? Wie und wann wurde der Vorfall festgestellt?
Was wurde bisher unternommen?

Informieren Sie die **Verantwortlichen.**

Kontaktieren Sie uns.
Tel.: **+49 421 69 66 32-0**
E-Mail: **forensik@datenschutz-nord.de**



01/dsn

datenschutz nord GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88
28217 Bremen
Tel.: +49 (0) 421 69 66 32-0

office@datenschutz-nord.de
www.datenschutz-nord-gruppe.de

datenschutz süd GmbH

Hauptsitz Würzburg
Wörthstraße 15
97082 Würzburg
Tel.: +49 (0) 931 30 49 76-0

office@datenschutz-sued.de
www.datenschutz-nord-gruppe.de

Weitere Niederlassungen der datenschutz nord Gruppe siehe **www.datenschutz-nord-gruppe.de/standorte**

datenschutz nord

datenschutz süd