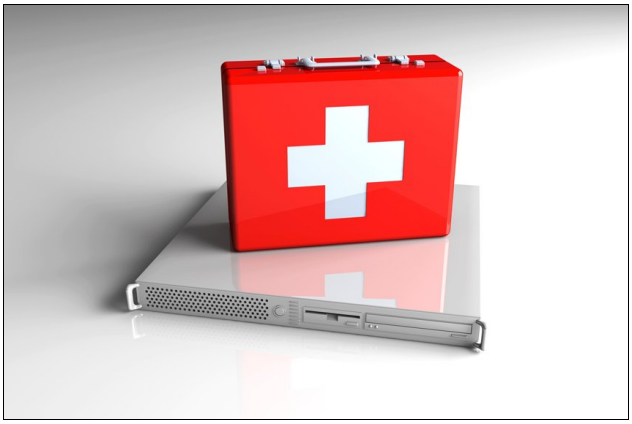
Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

IT-Sicherheitstipp: Notfallplan: Was tun, wenn es passiert ist?



Das regelmäßige Einspielen von Sicherheitsupdates und der Einsatz aktueller Virenschutzsoftware und einer Personal-Firewall finden immer häufiger Verwendung. *„Viele kleine Unternehmen haben die Notwendigkeit erkannt, in IT-Sicherheit zu investieren“*, so Sebastian Spooren vom Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen [1]. Ein technischer Basis-Schutz reicht jedoch nicht aus. Wenn plötzlich die Festplatte des Unternehmensservers versagt, kann der Schaden groß sein. Schlimmstenfalls bedeuten technische Defekte oder ein Datendiebstahl durch Kriminelle den Ruin des Unternehmens. Kommt es – trotz umfangreichen Sicherheitsvorkehrungen – zu so einem solchen Szenario, ist schnelles und überlegtes Handeln gefragt. Laut einer aktuellen Studie des *Bundesministeriums für Wirtschaft und Technologie* in Zusammenarbeit mit dem *Netzwerk Elektronischer Geschäftsverkehr* (kurz: *NEG*) besitzt nur jedes vierte Unternehmen konkrete Pläne für den Notfall Datenverlust. Ausgehend von dieser Studie, scheinen sich kleine und mittelständische Unternehmen großen Sicherheitsrisiken auszusetzen. So hat bereits jedes fünfte Unternehmen mindestens einmal einen unwiderruflichen Datenverlust erlitten [2]. Erfahren Sie in diesem Sicherheitstipp, welche entscheidenden Maßnahmen Sie im Notfall treffen sollten, um den wirtschaftlichen und informellen Schaden so gering wie möglich zu halten.

Kontaktieren Sie im ersten Schritt den IT-Sicherheitsbeauftragten

Sollten Sie Schwierigkeiten haben, gespeicherte Dateien und Dokumente zu öffnen oder wieder zu finden, kontaktieren Sie umgehend den IT-Sicherheitsbeauftragten [3] Ihres Unternehmens, ohne selbst Datenrettungsversuche zu unternehmen. Scheuen Sie sich nicht, auch bei kleineren Hard- oder Softwareproblemen an Ihren Kollegen heran zu treten. **Oft ist das Schadensausmaß eines Datenverlusts davon abhängig, wie schnell und ehrlich Schwierigkeiten kommuniziert werden.** Sollte in Ihrem Unternehmen bislang noch kein IT-Sicherheitsbeauftragter berufen worden sein, so informieren Sie sich mithilfe des IT-Sicherheitstipps *„Für den Datenverlust richtig vorbereitet sein“* [4] über notwendige Präventivmaßnahmen. Sobald der Beauftragte die Situation analysiert hat, kann er Maßnahmen zur Datenrettung und — sofern vorhanden — den betrieblichen Notfallplan einleiten und weitere Schritte

mit der Belegschaft abstimmen. Je nach Gefährdungslage sollte er in Kooperation mit der Unternehmensleitung und allen Beschäftigten ein Notfall-Meeting abhalten und Anweisungen geben. Die Unternehmensleitung sollte ihre Belegschaft zu hoher Kommunikationsbereitschaft bestärken, wenn es um das Thema IT geht. Wer häufig Probleme artikuliert, gilt keinesfalls als inkompetent, sondern vielmehr als sehr gewissenhaft in seinem betrieblichen Alltag.

Greifen Sie bei Virenbefall auf Backups zurück oder setzen Sie das System neu auf

Bevor Sie versuchen, verlorene oder beschädigte Dateien zu retten, sollten Sie Ihren PC keinesfalls neu starten, sondern zunächst eine Überprüfung Ihres gesamten Systems durch ein geeignetes und aktuelles Antiviren-Programm durchführen. Schlägt dieses Alarm und werden Schadprogramme wie Viren oder Trojaner gefunden, sollten Sie versuchen, diese mit Hilfe des Programms zu beseitigen (Tipps hierzu im IT-Sicherheitstipp *„Hilfe beim Virenbefall“* [4]). Anschließend sollten Sie alle persönlichen und unternehmensinternen Daten auf einem externen Medium sichern, um die aktuellen und virengeprüften Dateien später wieder zurück spielen zu können. **Da Sie nach dem Fund von Schadprogrammen nicht wissen, welcher Schaden an Ihrem System angerichtet wurde, ist das Einspielen einer kompletten Datensicherung oder eine Neuinstallation Ihres Systems und die Änderung sämtlicher Passwörter für diesen PC zwingend erforderlich.** Andernfalls laufen Sie Gefahr, dass die erkannten Schadprogramme zwar restlos entfernt worden sind, aber zwischenzeitlich Ihr System so verändert haben, dass Dritte nun unbemerkt Zugang zu Ihrem System erlangen können.

Setzen Sie Datenrettungs-Software wohl überlegt ein

Haben Sie keine Möglichkeit, Ihre dringend benötigten Dateien über Datensicherungen wieder zu gewinnen, besteht die Option, spezielle Datenrettungs-Software einzusetzen. Doch hier ist Vorsicht geboten: Sowohl kostenlose, als auch kostenpflichtige Software sollte generell nur dann eingesetzt werden, wenn sie aus seriöser Quelle stammt. **Nehmen Sie das jeweilige Produkt und den Hersteller genau unter die Lupe und vergleichen Sie unterschiedliche Produkte auf den Funktionsumfang hin.** Zudem ist eine Datenrettungs-Software nicht für jeden Anwender sinnvoll. Sind Sie Neuling im Umgang mit Software dieser Art, ziehen Sie einen IT-Fachmann zu Rate. Die Installation und der Einsatz spezieller Programme sollte gut überlegt sein. Es besteht ein großes Risiko, die Situation Ihrer Festplatte durch Softwareeingriffe dieser Art weiter zu verschlimmern, sodass spätere professionelle Datenrettungsversuche durch Dienstleistungsunternehmen nicht weiterhelfen können. **Bevor Sie eine Datenrettungs-Software einsetzen, sollten Sie deshalb immer mit einer Kopie Ihrer Festplatte arbeiten und niemals Datenrettungsversuche auf Ihrem Original-Datenträger durchführen lassen.**

Schalten Sie im Zweifelsfall einen Spezialisten ein

In manchen Fällen hilft nur noch die professionelle Hilfe eines seriösen Datenrettungs-Unternehmens. Mittlerweile hat sich eine eigene Branche auf diese Tätigkeit spezialisiert. Meist müssen Sie den gesamten Datenträger in die Hände der Spezialisten abgeben. **Wichtig ist, vorher unbedingt ein Abbild des darauf enthaltenen Inhalts zu erstellen.** Auch hierbei bekommen Sie im Zweifelsfall Hilfe von dem auf Datenrettung spezialisierten Unternehmen. Nachdem Sie einige Fragen zur Beschaffenheit Ihrer IT-Umgebung und zur Art der verlorenen oder beschädigten Daten beantwortet haben, erfolgen zahlreiche professionelle Datenrettungsversuche auf verschiedenen Wegen. Dabei wird je nach Art der beschädigten Daten, zum Beispiel durch Virenbefall oder Brand, die Datenrettung softwaretechnisch oder auf Hardware-Ebene durchgeführt.

Schalten Sie die Polizei ein, wenn der Verdacht auf Wirtschaftsspionage besteht

Sollten Sie starke Indizien dafür haben, Opfer von Wirtschaftsspionage geworden zu sein, so kappen Sie schnellstmöglich alle Internetverbindungen Ihrer im Netzwerk befindlichen PCs, um einen weiteren nicht autorisierten Zugriff durch Kriminelle zu verhindern. Allerdings sollte diesem Vorgehen ein konkretes Ereignis vorausgegangen sein, wie beispielsweise eine eindeutige Telefonattacke zum Zweck des Datendiebstahls, sogenanntes *Social Engineering*. **Melden Sie den Vorfall umgehend der Polizei — dies gilt natürlich auch bei einem Diebstahl eines Datenträgers.** Sollte sich der Tatverdacht erhärten, erstatten Sie bei der Polizei Anzeige. Eventuell müssen Sie den Beamten die betreffenden Datenträger oder PCs zur Verfügung stellen. Wie Sie sich in Zukunft vor Phishing und Social Engineering schützen können, erfahren Sie in der Informationsbroschüre *„Gefahr durch Social Engineering“* [4] und im *NEG-Awareness-Video „Wie schütze ich mich vor Phishing?“* [4]. **Lassen Sie anschließend Ihre IT-Umgebung von einem IT-Sicherheitsexperten auf Sicherheitslücken hin untersuchen.**

Autoren

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen

[2] http://www.kmu-sicherheit.de

http://www.ec-net.de

[4] http://ratgeber.it-sicherheit.de

[1] https://www.internet-sicherheit.de

[3] http://www.bsi-fuer-buerger.de

http://www.bitkom.de

http://www.sicher-im-netz.de

Bildquelle: © Spectral-Design - Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de