Cybercrime, also durchs Internet oder Netzwerke begangene Straftaten, sind längst fester, bedauerlicher Bestandteil unserer Gesellschaft geworden. Das Bundeskriminalamt veröffentlichte in seinem Bericht zur Bundeslage 2018 mehr als 87.000 Straftaten. Die Spielarten der Cyberkriminalität sind inzwischen sehr vielseitig und reichen vom Datendiebstahl bis hin zur digitalen Erpressung. Die Medien berichten inzwischen regelmäßig von Fällen, bei denen große Konzerne gehackt wurden – aber auch kleine und mittelständische Firmen sind beliebte Ziele für Angriffe, da Datenmaterial hier im Regelfall schlechter oder gar nicht geschützt ist. Die finanziellen Folgen eines solchen Angriffs können schnell in die Tausende gehen.

SCHADENBEISPIELE AUS DER PRAXIS

WAS KANN IHREM UNTERNEHMEN ZUSTOSSEN?

Da der Themenkreis „Cyber Risiken“ für viele noch in der Kategorie „böhmisches Dorf“ abgelegt ist, möchten wir an dieser Stelle gerne auf die häufigsten Schadensereignisse eingehen. Wir hoffen, dass Ihnen unsere Ausführungen auch Hilfestellung bieten, dieses Gefahrengebiet besser zu verstehen und das konkrete Gefahrenpotenzial für Ihr Unternehmen realistischer einschätzen zu können.

MAILBOMBE

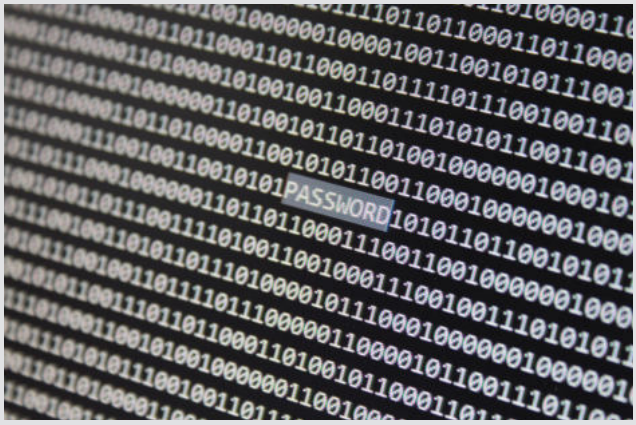
Unter einer Mailbombe versteht man das organisierte Verschicken einer Vielzahl von E-Mails (mit oder ohne Anhängen), um die E-Mail-Kommunikation des Empfängers zu blockieren. Inzwischen bietet das Internet eine Vielzahl frei downloadbarer Tools, über die es möglich ist, tausende von Mails gleichzeitig an einen Empfänger zu versenden. Dies führt – abhängig von Stückzahl und Mailgröße – zu immensen Verzögerungen im Arbeitsalltag. Nicht selten dauert es mehrere Stunden, bis alle Mails empfangen wurden und man sich wieder z. B. der Kommunikation mit Kunden zuwenden kann. Es ist zudem möglich, dass der Mailserver durch die Bombe überlastet wird und gar keine Mails mehr verarbeitet werden können.

Schadenbeispiel: Ein Callcenter wickelt u. a. für eine Direktbank die Kunden-, Telefon- und Mail-Hotline ab (First-Level). Ein Kunde der Bank startet aus Ärger über eine Anlageempfehlung eine Mailbombe, die aber natürlich beim Callcenter „einschlägt“ und die Mailkommunikation dort lahmlegt. Es vergehen zwei Tage, in denen keinerlei Mails beantwortet werden können. Es entstehen Kosten für die Untersuchung und Überstunden der Belegschaft zur Aufarbeitung des Rückstands.

DOS-ATTACKE (DENIAL OF SERVICE)

Denial of Service (kurz DoS; engl. für „Dienstverweigerung“) bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz verursacht werden. Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird von einer verteilten Dienstblockade oder Distributed Denial of Service (DDoS) gesprochen.

Schadenbeispiel: Ein mittelständischer Versand für Outdoor- und Military-Zubehör betreibt auch einen erfolgreichen Onlineshop, dessen Anteil am Gesamtumsatz über die Jahre auf 70 % anstieg. Bedingt durch das Sortiment machen ein paar studentische Aktivisten aus „dem linken Lager“ das Unternehmen als „Naziversand“ aus und starten über ein Bot-Net eine DDoS-Attacke, bei der der Shop tausende von Malen immer und immer wieder angefragt wird, bis der Server kapituliert. Da die Attacke über eine komplette Woche fortgesetzt wird, ist der Shop erst nach einigen technischen Änderungen wieder erreichbar. Die entstandenen Kosten: Technische Optimierung, Untersuchung, entgangener Umsatz für eine Woche, Imageschaden wg. Nichterreichbarkeit, etc.



DATENMISSBRAUCH

Datenmissbrauch hat ebenfalls viele Gesichter. Am häufigsten ist hier der betrügerische Missbrauch von Bank- und Kreditkartendaten der Kunden eines Unternehmens, da hiermit sehr schnell Geld ergaunert werden kann. Auch das Ausspionieren eines Unternehmens („Industriespionage“) fällt unter diese Kategorie der Cyber-Risiken. Zugang kann der Täter über Schadsoftware (z. B. Keylogger), Hardware (z. B. gestohlener PC) oder über Mitarbeiter (z. B. „geborgten“ Zugang) erhalten.

Schadenbeispiel: Die Kundendatenbank eines Autohauses wird gehackt. Dabei erbeuten die Täter u. a. sämtliche gespeicherten Kreditkartendaten der Kunden. Dem Autohaus entstehen Kosten für Forensik, technische Optimierung, Schadenersatzforderungen der betroffenen Banken, etc.

DATENSABOTAGE

Bei einem Datensabotageakt werden Daten beschädigt, verändert oder gelöscht. Dies kann über ein Schadprogramm erfolgen oder gezielt durch einen Eindringling vorgenommen werden.

Schadenbeispiel: Ein Auszubildender einer Werbeagentur nutzt seine Mittagspause dazu, im Betrieb einen Film herunterzuladen. Diesen legt er auf dem Firmenserver ab, wo ihn sich auch zwei Kollegen kopieren. Die Datei war mit einem Virus versehen, der beim Aufruf des Films die Computer befällt und sich über das Firmennetzwerk verbreitet. Der Virus löscht eine ganze Reihe von Dateien unwiederbringlich. Die Arbeit, die in diese Kundenaufträge investiert wurde, ist verloren - trotz angeordneter Überstunden können nicht alle Abgabetermine eingehalten werden. Es entstehen Kosten für die Forensik, technische Optimierung, Schadenersatzforderungen der Kunden, Kunden wandern ab und das Image der Firma hat schweren Schaden genommen.

DIGITALE ERPRESSUNG

Digitale Erpressung kann in verschiedenen Formen auftreten. Die größte Verbreitung findet über sog. „Ransomware“ statt, Schadprogramme wie z. B. der bekannte „BKA-Trojaner“. Hier wird in der Regel der Zugriff auf den eigenen Rechner blockiert und suggeriert, dass diese Blockade aufgehoben wird, wenn man eine Zahlung tätigt (z. B. als Bußgeld „getarnt“). Allerdings gibt es natürlich auch Fälle, in denen Firmen mit angedrohten DDoS-Attacken zur Lösegeldzahlung erpresst werden. Auch die Drohung, erbeutete Kundendaten zu veröffentlichen, etc. ist ein häufiger Erpressungsansatz.

Schadenbeispiel: Hackern gelingt es, Zugriff auf die Patientenakten eines Allgemeinmediziners zu erlangen. Nachdem die Datenbank erfolgreich kopiert wurde, schreiben sie den Praxisinhaber per Mail an und drohen mit der Veröffentlichung der Anamnesen – natürlich mit dem Vermerk, woher die Daten stammen. Gegen Zahlung einer gewissen Geldsumme via Western Union könne er die Veröffentlichung verhindern.