Schadenszenarien Cyber

Cybercrime ist längst fester Bestandteil unserer Gesellschaft geworden. Genauso wie die Angriffe auf Unternehmen zunehmen, vervielfachen sich auch die Spielarten der Cyberkriminalität. Wir stellen Ihnen hier typische Schadenszenarien vor und hoffen, dass Sie dadurch das konkrete Gefahrenpotenzial für Ihr Unternehmen realistischer einschätzen können:

	Eine Mailbombe meint das organisierte Verschicken einer Vielzahl von E-Mails mit oder ohne Anhängen, um die E-Mail-Kommunikation des Empfängers zu blockieren. Im Internet gibt es viele Tools zum freien Download, mit denen auch Laien tausende von Mails gleichzeitig an einen Empfänger versenden können. 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 der Kundenkommunikation zuwenden kann. Es ist zudem möglich, dass der Mailserver durch die Bombe überlastet wird und gar keine Mails mehr verarbeitet.	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.

	Denial of Service (kurz DoS; engl. für „Dienstverweigerung“) bezeichnet die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. In der Regel ist DOS 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, wird von einer Distributed Denial of Service (DDoS) gesprochen.	Schadenbeispiel Ein mittelständischer Versand für Outdoor- und Military-Zubehör betreibt einen Onlineshop. Bedingt durch das Sortiment starten ein paar Aktivisten über ein Bot-Net eine DDoS-Attacke, bei der der Shop so oft angefragt wird, bis der Server kapituliert. Da die Attacke über eine 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.
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 lädt im Betrieb ein Video auf den Firmenserver herunter. Mehrere Kollegen kopieren es. Die virusverseuchte Datei verbreitet sich über das Firmennetzwerk und löscht eine ganze Reihe von Kunden-aufträgen unwiederbringlich. Trotz Überstunden können nicht alle Abgabetermine eingehalten werden. Es entstehen Kosten für die Forensik, Schadenersatzforderungen der Kunden, Kunden wandern ab und das Image der Firma nimmt schweren Schaden.

	Beim Datenmissbrauch ist der betrügerische Missbrauch von Bank- und Kreditkartendaten der Kunden eines Unternehmens am häufigsten. Auch das Ausspionieren eines Unternehmens, die Industriespionage, fällt unter diese Kategorie der Cyber-Risiken. Zugang kann der Täter über Schadsoftware, Hardware (z. B. gestohlener PC) oder über die Mitarbeiter 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, Schadenersatz-forderungen der betroffenen Banken, etc.
	Digitale Erpressung kann in verschiedenen Formen auftreten. Die größte Verbreitung findet über Schad-programme (bspw. Ransomware) statt. Hier wird in der Regel der Zugriff auf den eigenen Rechner blockiert und suggeriert, dass diese Blockade aufgehoben wird, wenn man eine Zahlung tätigt. Allerdings gibt es 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 Hausarztes zu erlangen. Nachdem die Datenbank erfolgreich kopiert wurde, kontaktieren sie den Praxisinhaber per Mail 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.