Cyberkriminalität - Richtiges Verhalten bei IT-Sicherheitsvorfällen

IT-Sicherheit an der Universität Regensburg

Der Begriff „Cybercrime steht als international einheitliche Beschreibung für Computerkriminalität und umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese gegangen werden; am häufigsten unter Verwendung des Tatmittels Internet und E-Mail.

Cybercrime wird ein immer lukrativeres Geschäft. Nicht nur Weltkonzerne werden Opfer von Datenklau, Computersabotage oder Computerbetrug, sondern auch die Universitäten rücken immer mehr in den Fokus von Cyberkriminellen. Die Cyberkriminellen haben es heute nicht nur auf neue Entwicklung oder Wissensinterna abgesehen. Oft wollen sie den Betroffenen auch finanziell schaden oder das Image negativ beeinflussen.

Grundlagen für die Verfolgung von Cybercrime

Die folgende Darstellung gibt einen Überblick über die einschlägigen Strafbestände des Strafgesetzbuches (StGB):

Strafbestände	Inhalt (Kursbeschreibung)
§202a StGB Ausspähen von Daten 	Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung.
§ 202b StGB Abfangen von Daten 	Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln.
§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten 	Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist.
§ 202d StGB Datenhehlerei 	Das sich oder einem anderen Verschaffen, Überlassen, Verbreiten oder Zugänglichmachen von nicht allgemein zugänglichen und durch einen anderen aus einer rechtswidrigen Tat erlangten Daten mit der Absicht, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

§ 263a StGB Computerbetrug 	Das Schädigen des Vermögens eines Anderen durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf. Des Weiteren das Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Veräußerung, Verwahrung oder Überlassung eines Computerprogramms, dessen Zweck die Begehung einer solchen Tat ist.
§ 269 StGB Fälschung beweiserheblicher Daten 	Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, sodass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten.
§ 303a StGB Datenveränderung 	Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.
§ 303b StGB Computersabotage 	Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch 1. Begehung einer Datenveränderung (§ 303a), 2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen Nachteil zuzufügen, 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.

Grundlegende Tipps für den Arbeitsalltag

- Nehmen Sie das Schulungsangebot des RZ zum Thema IT-Sicherheit wahr.
- Halten Sie sich an die IT-Sicherheitsvorschriften Ihres Arbeitgebers, diese dienen Ihrem und dem Schutz der Universität.
- Seien Sie zurückhaltend mit der Weitergabe von vertraulichen und persönlichen Informationen.
- Haben Sie ein gesundes Misstrauen und scheuen Sie sich nicht vor persönlichen Rückfragen, wenn Ihnen etwas ungewöhnlich vorkommt.
- Überprüfen Sie E-Mails auf die richtige Absenderadresse sowie die korrekte Schreibweise der E-Mail-Domain.
- Öffnen Sie keine verdächtigen Mails.
- Seien Sie misstrauisch bei Links oder Anlagen in E-Mails unbekannter Absender.

Handlungsempfehlungen bei Betroffenheit von Cybercrime-Delikten

Die nachfolgenden Informationen sollen Ihnen Ratschläge und Tipps an die Hand geben, wie Sie sich im Schadensfall verhalten sollten.

Reagieren Sie sofort bei Verdacht

Bei einem Verdacht auf eine Cyberattacke sammeln Sie alle Informationen zum Vorfall und lassen diese aufzeichnen.

Melden Sie den Angriff früh dem IT-Sicherheitsbeauftragten

Empfehlenswert ist es sich an den IT-Sicherheitsbeauftragten des RZ der Universität Regensburg zu wenden. Dieser nimmt eine erste Beurteilung vor und nimmt gegebenenfalls Kontakt mit den Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC) auf.

Wenden Sie sich an:

Rechenzentrum Universität Regensburg
IT-Sicherheitsbeauftragte
Elena Maria Kellinghaus
Universitätsstraße 31
D- 93053 Regensburg
Telefon: +49 941 943 4889
Elena.Kellinghaus@rz. uni-regensburg.de

Rechenzentrum Universität Regensburg
IT-Sicherheitsbeauftragter
Klaus Schmidt
Universitätsstraße 31
D- 93053 Regensburg
Telefon: +49 941 943 4606
Klaus.Schmidt@rz.uni-regensburg .de

UR Internetpräsenz zur IT-Sicherheit und Datenschutz:
www.uni-regensburg.de/informationssicherheit