e-Crime

e-Crime (Computerkriminalität) bezeichnet die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde.
Dazu zählen zum Beispiel die Sabotage an Computersystemen, der Diebstahl von Quellcode und Kundendaten sowie die Beeinträchtigung von auf Systemen basierenden Geschäftsprozessen. Kommunikationssysteme können sowohl Ziel als auch Tatwerkzeug an sich sein. Im Gegensatz zu Cybercrime umfasst e-Crime nicht nur Angriffe von außen unter Nutzung von Schadsoftware oder Systemlücken über das Internet, sondern auch den internen Täter sowie weitere Möglichkeiten der Informations- und Kommunikationstechnologie als Werkzeug.

Studie zur Computerkriminalität

Zum zweiten Mal hat das Wirtschaftsprüfungsunternehmen KPMG eine umfassende Untersuchung zum Thema Computerkriminalität durchgeführt und dafür Führungskräfte aus 500 deutschen Unternehmen unterschiedlicher Größen und Branchen durch das Sozialforschungsinstitut TNS Emnid befragen lassen. Die e-Crime Studie 2013 zeigt, dass ein Viertel der befragten Unternehmen in den vergangenen zwei Jahren Opfer von e-Crime war. Am häufigsten kamen Computerbetrug und das Ausspähen oder Abfangen von Daten vor. 75 Prozent der Delikte wurden von unbekannten Externen begangen – eine deutliche Verschiebung gegenüber der Vorgängerstudie, als aktuelle oder ehemalige Mitarbeiter die größte Tätergruppe darstellten. 85 Prozent der betroffenen Unternehmen gaben an, dass die Angriffe immer komplexer werden. Durch die zunehmende Verbreitung mobiler Telekommunikation seien die Täter zudem schwerer zu identifizieren.

Aufdeckung und Prävention

Eine große Rolle bei der Prävention von e-Crime spielt die Kooperation zwischen Polizei und Wirtschaftsunternehmen. Laut BKA ist eine Zusammenführung von Erkenntnissen und somit ein koordiniertes Vorgehen gegen Tätergruppierungen, die oftmals mit dem gleichen Geschäftsmodell eine Vielzahl von Wirtschaftsunternehmen angreifen, nur dann möglich, wenn die Polizei über diese Vorgänge informiert wird. Außerdem kann sie so Unternehmen für Gefährdungslagen besser sensibilisieren und Präventionsarbeit leisten. Die e-Crime-Studie ist für die Polizei ein weiterer Indikator, ob und inwieweit Empfehlungen zur Prävention durch die Wirtschaft aufgegriffen werden und wo eine Kooperation zwischen Sicherheitsbehörden und Wirtschaftsunternehmen zur Bekämpfung geboten scheint. Es zeigt sich, dass die betroffenen Unternehmen in erster Linie durch offene Hinweise von Unternehmensexternen, wie Kunden, Lieferanten und sonstigen Geschäftspartnern (54 Prozent), erstmalig von in ihrem Unternehmen begangenen e-Crime-Handlungen erfahren haben. Damit spielen die Unternehmensexternen, ebenso wie Strafverfolgungs- beziehungsweise Regulierungsbehörden (31 Prozent), bei der Erkennung von e-Crime insgesamt eine wesentlich größere Rolle als noch 2010.

Siehe auch:
Wirtschaftskriminalität
Allianz für Cyber-Sicherheit

Zurück