

Forensic Accounting

e-forensic

Computer Kriminalität

Es besteht weltweit Uneinigkeit darüber, was unter Computer-Kriminalität überhaupt zu verstehen ist. Ist es ein Verbrechen, wenn man bei einem Freund ein Programm ausleiht und es auf seinem eigenen Computer installiert? Oder ist es strafbar, wenn man in ein anderes System eindringt und dort Schaden anrichtet? Wie steht es mit dem absichtlichen Verbreiten von Viren? Es gibt keine allgemein gültigen Antworten auf diese Fragestellungen, weil sie von verschiedenen Umständen und Strafnormen abhängen.

Man kann drei Arten von Computer-Kriminalität unterscheiden:

- Der Computer ist das Ziel.
- Der Computer ist das Tatwerkzeug.
- Der Computer spielt eine zufällige Rolle.

Ein Computer ist dann das Ziel, wenn ein Rechner oder Komponenten davon von einem anderen System mit krimineller Absicht angegriffen oder darin eingedrungen wird (z. B. Sabotage, Computerspionage, Raub, Betrug, Erpressung etc.).

Von einem Computer als Tatwerkzeug kann man insbesondere dann sprechen, wenn eine eigentlich konventionelle Tat unter Mithilfe eines Computers begangen wird (z. B. Fälschen von Banknoten oder anderen Dokumenten mit Scannern und Farbdruckern, Belästigung mittels Mailbomben oder Drohbrieffen, Verteilung oder Speiche-

rung von pornografischem Material, Glücksspiele, etc.).

Eine zufällige Rolle spielt ein Computer dann, wenn er für die Tat eigentlich nicht notwendig wäre (z. B. Drohbrieffe mit Computer geschrieben und per Post versandt, Buchhaltungen von illegalen Tätigkeiten mit einem Computer erstellt, etc.).

Täter

Um eine Straftat aufzuklären, ist es nötig, ein Profil des Täters zu erstellen. Im Falle von Computerdelikten ist dies nicht anders. Allgemein gültige Regeln für das Erstellen eines Täterprofils gibt es aber nicht. Wer ist der typische Hacker? Welches ist das "normale" Profil eines Betrügers? Wer kauft Programme?

Heutzutage kann fast jeder Schüler ab einem bestimmten Alter mit Computern umgehen und weiss, wie das Internet funktioniert. Anleitungen zu Hacking oder zum Schreiben von Viren findet man ohne Probleme. Raubkopien von Programmen sind auf dem Netz ebenso verfügbar, wie Informationen über die Herstellung von Mailbomben.

Einige allgemeine Feststellungen zum Profil des Täters lassen sich aber machen:

1. Gemäss verschiedenen Studien sind über 80% der Täter Insider.
2. Das Know-how ist bei jüngeren Tätern in der Regel grösser.

3. Raum und Zeit spielen eine untergeordnete Rolle.
4. Ein besonderes Augenmerk ist auf die hausinternen Informatiker zu richten (sie haben in der Regel auf *alle* Daten einer Firma unbeschränkt und *unbemerkt* Zugriff)
5. Outsourcing von EDV-Leistungen müssen speziell beurteilt werden und bieten zusätzliche Angriffspunkte.

Aufklärung

Im e-forensic-Bereich können folgende Tätigkeiten unterschieden werden:

Vorbeugung

- Aufzeigen der Bedrohung und der Eintrittswahrscheinlichkeit unter Berücksichtigung des zu schützenden Systems.
- Überprüfung der getroffenen Massnahmen im organisatorischen, baulichen und logischen Bereich.
- Sensibilisation der Führungskräfte (insbesondere derjenigen, die nichts von Informatik verstehen).
- Überprüfen der Notfall- und Katastrophenfallplanungen.
- Bildung eines Emergency-Teams.
- Sicherheitsprüfungen (Penetrationstest etc.).
- Dauernde Überwachung von sensiblen Systemen.

Motto: Vorbeugen ist besser als heilen!

Aufklärung

- Feststellung und Verfolgung von Eindringversuchen (Backtracking) – diese Methode funktioniert allerdings

nur, wenn entsprechende Vorbereitungsmaßnahmen getroffen wurden!

- Spurensicherung
- Überprüfen von Berechtigungen
- Beweismittelsicherung
- Datenrekonstruktion
- Auswertung von Daten (auch Mas-sendaten)

Repression

- Expertisen zu Händen der Untersuchungsorgane und Gerichte.

Probleme

Probleme bei der Aufklärung von Computerdelikten bieten neben der Tatsache, dass entsprechende Fachspezialisten rar sind auch rechtliche Schranken. Strafverfolgungsbehörden sind auf langwierige Rechtshilfverfahren mit dem Ausland angewiesen. Hacker überqueren in Sekundenbruchteilen Kontinente...

Viele der Betroffenen überlassen das Problem den eigenen Informatikern. Gründe dafür sind Angst vor Imageverlust, Unwissen oder Desinteresse der Geschäftsleitung. Die Informatiker sind selbst aber potentielle Täter...

Rolf Schatzmann (47) leitete während 12 Jahren den Sicherheitsdienst der Bundesverwaltung. In dieser Funktion war er nicht nur für Belange des Personenschutzes, sondern auch für den Objekt- und Informationsschutz der allgemeinen Bundesverwaltung zuständig.

Heute ist er Partner der Firma Ernst&Young AG in Zürich und leitet

dort den Geschäftsbereich Forensic Services Schweiz. Dieser Bereich bietet umfassende Dienstleistungen im Bereich Sicherheit an. Dazu gehören Untersuchungen bei vermuteten und bestätigten Unregelmässigkeiten, Prävention von Wirtschaftskriminalität sowie die Beratung in Compliance- und Integrity-Fragen. Als Spezialgebiet sind die Forensic Services im IT-Umfeld tätig. Diese Tätigkeiten umfassen Beratung in Sicherheitsfragen, Notfallkonzepte und Abklärungen nach erfolgten Zwischenfällen (Fraud, Hacking etc.).

Résumé: e-forensic

La criminalité informatique est une branche nouvelle dont l'étude implique quelques définitions préalables. Il ne suffit par exemple pas qu'une lettre de menace soit écrite à l'aide d'un programme de traitement de texte ou

que des billets de banque soient falsifiés à l'aide d'un scanner pour que l'on soit en présence d'un cas de criminalité informatique.

Le profil des auteurs de cette nouvelle forme de criminalité présente également des particularités : internes à l'entreprise ou éventuellement employés par un outsourcer, qualifiés et en général jeunes.

Point commun avec la criminalité classique : *prévenir vaut mieux que guérir*. Dans le domaine informatique, la répression se heurte en effet très rapidement aux obstacles géographiques et politiques : les délits sont commis internationalement mais sont réprimés par les polices nationales qui ont beaucoup de peine à intervenir au-delà de leurs frontières. Le manque de spécialistes capables de réunir et de traiter de manière appropriée les éléments de preuve vient encore assombrir le tableau.

Forensic Accounting

Reconnaître les indicateurs de fraude

Selon Donald G. Fulwider, directeur adjoint, Bureau des enquêtes spéciales, U.S. General Accounting Office.

■ Une gestion faible

Le fait que les contrôles existants ne soient pas appliqués, que la surveillance du processus de contrôle soit inadéquate et l'absence de mesures préventives sont signes d'une gestion faible.

■ Des contrôles internes faibles

La séparation inadéquate des tâches touchant la gestion de la trésorerie, les inventaires, les achats/les contrats, et les systèmes de paiement permettent à l'auteur de commettre des fraudes.

■ Des antécédents d'actes irréguliers

Les vérifications et enquêtes passées ayant révélé des activités douteuses ou criminelles sont très utiles et peuvent

servir de guide pour savoir où trouver les fraudeurs.

■ *Un leadership non éthique*

Les cadres qui ne respectent pas les règles et mettent l'accent sur les réalisations personnelles au lieu des objectifs de l'organisation peuvent être impliqués dans des activités frauduleuses.

■ *La promesse de gain et une faible probabilité de se faire prendre*

Quand une personne travaille dans un environnement où la gestion est faible, où les contrôles internes sont faibles et où il y a un gros volume de transactions, elle a d'amples possibilités d'exploiter la situation à son avantage personnel.

■ *Des décisions ou opérations non expliquées*

Des opérations qui sortent de l'ordinaire et qui ne sont pas expliquées de façon satisfaisante, par exemple, des redressements non expliqués aux inventaires et aux débiteurs, sont souvent signes d'activités frauduleuses.

■ *Le non-respect des conseils juridiques ou techniques*

Un écart non expliqué par rapport à un avis juridique ou technique, particulièrement quand la concurrence est exigée, peut être un signe de fraude.

■ *Des données modifiées ou des documents manquants*

Il arrive que l'auteur saisisse de façon délibérée des données fausses dans les fichiers ou supprime des données, en tentant de camoufler ces mutations. Constituent des indicateurs : des données manquantes, des données saisies longtemps après le fait générateur, des journaux de mutations ou des listes d'erreurs introuvables, ainsi que des différences entre les totaux recalculés et les totaux comptabilisés à des dates antérieures.

Forensic Accounting

Wirtschaftskriminalität/Korruption in der Bundesverwaltung

Faktoren, welche dolose/kriminelle Handlungen begünstigen

■ *Mangelnde Kontrolle durch Vorgesetzte*

Blindes Vertrauen, eingeschränkte Kontrollmassnahmen gegenüber besonders "guten", langjährigen Mitarbeitern, Gutgläubigkeit, Einräumung weitgehender Freiheiten, Vernachlässigung der Führungsverantwortung.

■ *Weitreichende finanzielle Kompetenzen*

Bedeutende Finanztransaktionen, Vertragsabschlüsse, Bewilligungen.

■ *Konzentration finanziell erheblicher Entscheide auf Einzelpersonen*
Z. B. im Beschaffungswesen, bei Subventionen, Projektleitungen, mit gleichzeitig fehlendem 4-Augen-Prinzip, bzw. fehlender Aufsicht (= Risikopotential für passive Bestechung).

■ *Fehlende Trennung der Funktionen*

Entscheidung, Vollzug, Verwaltung, Buchführung und Kontrolle, resp. Funktionenkumulation.

■ *Weitere Lücken im internen Kontrollsystem eines Amtes*

Z. B. fehlende Regelung von Arbeitsabläufen, keine systematisch eingebauten Kontrollen, "Eigenleben" einzelner Abteilungen oder Dienste.

■ *Lücken bei finanziellen Kontrollen*
Fehlende oder ungenügende Unterschriften-, Budget-, Abrechnungskontrollen im Finanz- und Rechnungswesen, wegen Personalengpässen nicht durchgeführte Kontrollen, zwar vorge-

sehene, aber aus verschiedenen Gründen nicht durchgeführte oder vernachlässigte Kontrollen.

■ *Uneingeschränkte Zugriffsberechtigung auf Informatikanwendungen*
Möglichkeit zur Datenentwendung, -zerstörung, -manipulation, Umgehung von automatisierten Kontrollen.

■ *Fehlende Kontrolle über Zugriffsberechtigungen und Zugriffen*
Keine oder ungenügende Verwaltung der Berechtigungen und Zugriffe.

■ *Nicht transparentes oder unübersichtliches Rechnungswesen*
Abwicklung eines Geschäftes über verschiedene Kredite, komplizierte Zahlungsabläufe, nicht autorisierte Bankkonti ausserhalb der Rechnung des Bundes.

Zur Verfügung gestellt von Michel Huissoud