

Diebstahl der Hardware

Zusammenfassung

Ein Dieb bemächtigt sich fremden Guts mittels Gewalt oder ohne das Wissen der bestohlenen Person. Alle Bestandteile eines EDV-Systems können Gegenstand eines Diebstahls sein. Diese Diebstähle können in den Räumen des Unternehmens

oder während des Transports der Hardware erfolgen. Ebenso wie der Diebstahl kann auch der Verlust von EDV-Geräten weitreichende Konsequenzen für die betroffene Person haben.

Inhalt

- 1 Was versteht man unter Diebstahl? →
- 2 Welche Komponenten sind betroffen? →
- 3 Grundlagen für die Einschätzung der Schäden →
- 4 Statistische Ergebnisse →
- 5 Welche Sicherheitslücken treten am häufigsten auf? →
- 6 Vorbeugende Maßnahmen →



1 Was versteht man unter Diebstahl?

Ein Dieb bemächtigt sich fremden Guts mittels Gewalt oder ohne das Wissen der bestohlenen Person. Alle Bestandteile eines EDV-Systems können Gegenstand eines Diebstahls sein.

Diese Diebstähle können in den Räumen des Unternehmens oder während des Transports der Hardware erfolgen. Ebenso wie der Diebstahl kann auch der Verlust von EDV-Geräten weitreichende Konsequenzen für die betroffene Person haben.

2 Welche Komponenten sind betroffen?

Es können verschiedenste Komponenten gestohlen werden bzw. verloren gehen, und daher ist es fast unmöglich, eine umfassende Liste aufzustellen.

Am häufigsten werden die nachfolgend aufgeführten Geräte gestohlen:

2.1 Portable Computer

Der beträchtliche Marktwert, eine hohe Speicherkapazität sowie die Miniaturisierung der portablen Computer haben diese Geräte in Bezug auf Diebstähle zu einem begehrten Objekt gemacht.

2.2 Personal Assistants (PDA - Personal Digital Assistant)

Aufgrund ihrer Miniaturisierung und Effizienz sind Personal Assistants eine begehrte Hehlerware. Die hohe Speicherkapazität der Personal Assistants kann sich im Fall eines Datenverlusts oder -diebstahls als eine bedeutende Quelle erweisen.

2.3 Magnetische oder optische Datenträger

Der Diebstahl dieser Datenträger ist vielleicht weniger bekannt und auf den ersten Blick auch weniger dramatisch, kann aber verhängnisvolle Konsequenzen für das betroffene Unternehmen haben. Der Diebstahl von magnetischen Datenträgern (Magnetbänder, Disketten) oder optischen Datenträgern wie etwa einer CD (Compact Disk), DVD (Digital Versatile Disk), eines USB-Speichers (Universal Serial Bus) oder eines PCMCIA-Speichers (Personal Computer Memory Card International Association), die als Sicherheitskopie, Hauptspeicher oder Sicherungsspeicher (Backup) genutzt werden, kommt ziemlich häufig vor und ermöglicht den Diebstahl großer Datenmengen.

2.4 Mobiltelefone

Angesichts der zahlreichen Synchronisationsfunktionen zwischen den Mobiltelefonen und den EDV-Lösungen müssen diese Geräte eindeutig als ein Glied in der Kette der elektronischen Datenverarbeitung angesehen werden.

Diebstahl der Hardware

3

Grundlagen für die Einschätzung der Schäden

Der Diebstahl von EDV-Geräten kann schwerwiegende Folgen haben. Folgende Schäden können auftreten:

3.1 Wert des Gerätes oder Datenträgers

Bei einem Diebstahl eines Gerätes oder Datenträgers ist der unmittelbare Schaden der finanzielle Verlust, der den Kosten für die Wiederanschaffung des entwendeten Geräts entspricht.

Bei einem Diebstahl eines Mobiltelefons kommen möglicherweise noch die Gebühren für die Telefonate hinzu, die der Dieb vor der Sperrung des Mobiltelefons durch den Dienstanbieter tätigt.

3.2 Datenverlust/-diebstahl

Der Diebstahl oder Verlust eines Geräts kann abhängig vom Verwendungszweck des gestohlenen oder verloren gegangenen Geräts verschiedenste Auswirkungen mit beträchtlichen Schäden wie beispielsweise den Verlust von Know-how, das Ausspionieren von Fabrikationsgeheimnissen, die Verbreitung vertraulicher Daten, den Verlust des Ansehens der betroffenen Person, den Verlust von Finanzdaten, den Verlust von logischen Zugangscodes etc. haben.

Die Schäden für die betroffenen Personen können je nach Verwendungszweck der Hardware ganz verschiedenartig sein (Neuformatierung, um eine andere Nutzung zu ermöglichen, Nutzung zum unbefugten Eindringen in ein Netzwerk oder Verkauf von Daten).

3.3 Softwarediebstahl

Der Diebstahl von portablen Geräten beinhaltet logischerweise auch den Diebstahl aller auf diesem Gerät installierten Softwareprogramme.

Dies umfasst alle marktüblichen Softwareprogramme, aber auch spezielle für die Zwecke der Privatperson, des Unternehmens oder der Verwaltung entwickelte Softwareprogramme.

3.4 Netzwerkzugang

Der Diebstahl von Geräten, mit denen über die Technik der drahtlosen Netzwerke, per Infrarottechnik oder per Fernzugriff eine Verbindung zu einem Netzwerk oder anderen Peripheriegeräten hergestellt werden kann, ermöglicht den unbefugten Zugang zum Netzwerk der betroffenen Person. Dieser Zugang kann verwendet werden, um sich weitere Informationen zu bemächtigen oder weitere Schäden anzurichten.

3.5 Produktivitätsverlust

Die Nichtverfügbarkeit dieser Geräte versetzt das unglückliche Opfer häufig in die Lage, nicht mehr arbeiten zu können. Dieser mit dem Verlust von Dokumenten und Anwendungen verbundene Produktivitätsverlust kann zu einem enormen Arbeitsaufwand allein für die Wiederherstellung der Daten und Softwareprogramme in den Zustand, in dem sie sich zum Zeitpunkt des Diebstahls oder Verlusts befunden haben, führen. Dieser Arbeitsaufwand ist um ein Vielfaches höher, wenn die betroffene Person nicht über aktuelle Sicherungskopien verfügt.

3.6 Aufhebung der Intimssphäre

Es ist sehr wahrscheinlich, dass der Dieb, wenn er über minimale EDV-Kenntnisse verfügt, in der Lage ist, Softwareprogramme wie beispielsweise die e-Mail oder e-Banking-Anwendungen zu nutzen und sich dabei als der rechtmäßige Eigentümer auszugeben. Es liegt auf der Hand, dass in einem solchen Fall der finanzielle Schaden schnell beträchtliche Summen erreichen kann.

4

Statistische Ergebnisse

Zahlreiche Quellen liefern Informationen, die das Ausmaß des Diebstahls von EDV-Geräten beschreiben:

- ➔ Der Diebstahl von portablen Computern ist nach dem Versand von Viren das zweithäufigste Delikt im EDV-Bereich. (Studie des CSI/FBI (Computer Security Institute/Federal Bureau of Investigation) über Verbrechen und EDV-Sicherheit aus dem Jahr 2003).
- ➔ 591.000 portable Computer wurden während des Jahres 2001 in den Vereinigten Staaten entwendet (Time Magazine 27.01.03).
- ➔ Während des ersten Halbjahres haben eilige Reisende 62.000 Mobiltelefone, 2.900 portable Computer und 1.300 Personal Digital Assistants in den Londoner Taxis vergessen (BBC, August 2001).
- ➔ In Südkorea werden jährlich 2,8 Millionen Mobiltelefone verloren oder geklaut (Financial News, August 2002).

- ➔ IT-Sicherheitsbeauftragte gaben an, dass 57% der ausgenutzten Sicherheitslücken auf den Diebstahl von portablen Computern zurückzuführen sind (Studie des CSI).
- ➔ 70 % der Diebstähle von Computern erfolgen unternehmens- oder verwaltungsintern (Gartner Group).
- ➔ Der Diebstahl von portablen Computern stellt ein bedeutendes Risiko dar, da sensible Unternehmensdaten betroffen sind, und die Situation kann sich mit der zunehmenden Verwendung von so genannten Pocket-Geräten nur verschlimmern. Chris Christaensen, IDC (International Data Corporation).
- ➔ 33% aller Anwender von Personal Digital Assistants (PDA) nutzen diese Geräte zur Speicherung von Passwörtern und Zugangscodes, 25 % speichern dort kritische berufliche Daten und ebenfalls 25% speichern in diesen Geräten Daten bezüglich ihrer Bankkonten. (PointSec 's Survey).

Diebstahl der Hardware

5

Welche Sicherheitslücken treten am häufigsten auf?

Es ist leider nicht möglich, alle Sicherheitslücken zu schließen, aber man muss versuchen, die möglichen Auswirkungen mittels Kontrollen, Schutzmaßnahmen und Erkennungsmechanismen einzuschränken.

➔ Zugangssicherheit

Es muss eine effiziente Kontrolle des Zugangs zu Büros und Rechenzentren eingerichtet werden. Leider wird der physikalische

Zugang häufig nur unzureichend verwaltet. Die Verwaltung des Fernzugriffs muss strengstens überwacht und kontrolliert werden.

➔ Menschliche Fehler

Statistiken belegen, dass menschliche Fehler, mangelnde Vorsorge, Nachlässigkeiten, Verluste und Versäumnisse immer noch am häufigsten zu einem Verlust von EDV-Geräten führen.

6

Vorbeugende Maßnahmen

Es muss zwischen vorbeugenden Maßnahmen, deren Ziel es ist, derartige Ereignisse zu vermeiden, und den anderen Maßnahmen, deren Ziel die Erkennung und die Kontrolle dieser Art von Ereignissen bzw. die Einschränkung der Auswirkungen ist, unterschieden werden.

6.1

Die Verfahren

Das Vorhandensein, die interne Verbreitung, die Einhaltung und die Überwachung von Verfahren hinsichtlich der Verwendung, des Transports und der Lagerung von Datenträgern ermöglichen Ihnen, den Verlust bzw. den Diebstahl von Datenträgern in erheblichem Maß zu verringern.

Die Existenz und die Einhaltung von im Fall eines Datendiebstahls oder -verlusts zu befolgenden Verfahren wie beispielsweise die Filterung des Zugangs zu einem Netzwerk auf der Basis der MAC-Adresse (Media Access Control), die Unterbindung des Fernzugriffs, die Sperre des Kunden-VPN (Virtual Private Network) oder die Änderung aller Passwörter des Anwenders sind unumgängliche Maßnahmen zur Einschränkung der Auswirkungen.

> Diese Schutzmaßnahmen können nicht als vorbeugende Maßnahmen betrachtet werden, selbst wenn ihre Existenz und ihre Verbreitung vor einem internen Diebstahl abschrecken mögen.

6.2

Verwaltung des Hardware-Inventars

Nur die detaillierte Überwachung des Inventars ermöglicht es Ihnen, den Fernzugriff mittels gestohlener Geräte zu verhindern, und kann Ihnen als Grundlage für die Verhandlungen mit dem Versicherer dienen.

6.3

Einschränkung der Nutzung externer Datenträger

Die Anzahl der Diebstähle oder Verluste von Datenträgern (Disketten, CD ROM - Compact Disk Read Only Memory - etc.) ist proportional zur Anzahl der in Umlauf befindlichen Datenträger. Es kann sich daher als vorteilhaft erweisen, die Verwendung dieser Datenträger erstens einzuschränken und zweitens zu kontrollieren.

6.4

Verwendung von Vorhängeschlössern

Die Sperrung gewisser Peripheriegeräte wie beispielsweise der USB-Ports (Universal Serial Bus) oder der Infrarotschnittstellen kann die unbefugte Nutzung bestimmter Datenträger verhindern.

> Diese Schutzmaßnahme kann als vorbeugend eingestuft werden.

6.5

Verschlüsselung der Daten

Es wird dringend geraten, spezielle Softwareprogramme zur Verschlüsselung der auf der Festplatte der portablen Computer gespeicherten Daten zu verwenden. Diese Tools machen die Verwendung der gestohlenen Daten nahezu unmöglich.

> Diese Schutzmaßnahme kann als vorbeugend eingestuft werden.

6.6

Schutz per Passwort

Verwenden Sie wie in allen anderen Bereichen der EDV auch leistungsfähige Passwörter und löschen Sie unnötige Benutzerkonten auf dem Gerät.

> Diese Schutzmaßnahme kann als vorbeugend eingestuft werden.

6.7

Kennzeichnung der Geräte

Ganz gleich ob per Aufkleber oder Gravur - die Kennzeichnung der EDV-Geräte ist ein wichtiges Mittel, um einen Dieb von seinem Vorhaben abzubringen.

> Diese Schutzmaßnahme kann als vorbeugend eingestuft werden.