Workshop: IT-Security & Safety

Thomas HRDINKA

Ziviltechniker Dipl.-Ing. Thomas Hrdinka, ZTH Consulting Engineering, Weinbergg. 1d, 2202 Königsbrunn/Wien,
thrdinka@aon.at, http://www.zth.at

1 KURZBESCHREIBUNG

Fragen der IT-Sicherheit, der Datenintegrität und Vertraulichkeit der zu verarbeitenden Daten im Planungs- und Vermessungsbereich sollen nach einem kurzen einführenden Vortrag aufgezeigt und ausführlich diskutiert werden.

2 MOTIVATION

Es ist erstaunlich, daß unsere Rechner bereits mehr als 15 Jahre lang durch periodische Wellen von Vireninfektionen lahmgelegt werden. Trotz unablässiger Anstrengungen gegen diese Plage mit zum Beispiel Anti-Virus Software, Trojan-Scannern, Firewalls, Intrusion Detection Systemen, etc. gelingt es immer mehr, mittlerweile nicht nur tausende, sondern Millionen von Computern weltweit innerhalb weniger Stunden zu sabotieren – wie kann es dazu kommen, wie kann man sich schützen?

Auch moderne Planungs- und Vermessungsbüros müssen sich immer häufiger mit dieser Problematik beschäftigen; vielmehr, daß solche Unternehmen bereits fast vollständig von der EDV abhängig sind. Ein Rückschritt zwecks Problemvermeidung in die Zeiten ohne EDV kommt aus wettbewerbstechnischen Gründen nicht in Frage; zusätzlich könnte eine erfolgreiche Attacke auf die Computer so eines Büros existenzbedrohend werden – welche Maßnahmen sind nun zu treffen?

Über die Konsequenzen nicht rechtzeitig eingeführter, dem Stand der Technik entsprechender Schutzmaßnahmen, sollte sich jeder Inhaber eines Büros als auch der EDV-Verantwortliche im Klaren sein: Haftungsfragen, Wettbewerbsnachteile, oder sogar Strafbarkeit können zu den unangenehmsten Begleiterscheinungen zählen.

Computer-Security definiert die EDV-Sicherheit im vorher beschriebenen Sinn. Unter Computer-Safety versteht man unter anderem den Datenschutz, wie zum Beispiel Sicherung und Archivierung der Daten. Gerade diese Archvierungsproblematik, welche die Wahl von geeigneten Datenformaten und Speichermedien umfaßt, kombiniert mit einer gerade im Bau- und Vermessungswesen geltenden dreißigjährigen Aufbewahrungspflicht, stellen Inhaber von Planungsbüros vor nahezu unlösbare Probleme. Nachdem sich Haftpflichtversicherungen bei grober Fahrlässigkeit gerne leistungsfrei sehen, kann diese Problematik ein unkalkulierbares Risiko für jedes Unternehmens in der Zukunft bedeuten.

Ein weitere in diesem Zusammenhang nicht zu unterschätzende Problematik ist die Frage der Datenintegrität. Es ist, wie schon erwähnt, durchaus wichtig und zweckmäßig die Nettodaten zu sichern und zu archivieren, jedoch müssen diese interpretierbar bleiben. Wesentlich ist hier, daß sowohl der logische Zusammenhang der Datensätze erhalten bleibt, und daß die sogenannten Metadaten, die für die korrekte Interpretation dieser Daten zuständig sind, ebenfalls in die Zukunft gerettet werden.

Zum Schluß, nachdem viele technische und organisatorische Fragen, die im Zusammenhang mit der IT-Sicherheit stehen, angerissen worden sind, bleibt nur noch ein Restrisiko zu diskutieren: der Mensch. Da das Ausspähen von Informationen im Geschäftsleben immer lukrativer, und vor allem durch die hohe Datenkonzentration und Systemvernetzung, immer einfacher wird, müssen hier ebenfalls technische und organisatorische Maßnahmen getroffen werden, um die Vertraulichkeit der Daten zu gewährleisten.

In der Folge werden drei Themenschwerpunkte des Workshops genauer behandelt, um vorab einen Überblick in die Marterie zu erhalten.

3 IT-SICHERHEIT

Der etwas undeutliche Begriff der IT-Sicherheit umfaßt im Wesentlichen die beiden englischen Begriffe IT-Security und IT-Safety. Die IT-Security behandelt Fragen des Schutzes vor unberechtigtem Zugriff, Veränderung oder Löschung von Daten, somit Sicherheit vor beabsichtigten Störungen. Die IT-Safety definiert hingegen die Fragen der Sicherung und Archivierung, also Sicherheit vor unbeabsichtigten Schäden, wie Headcrashes, Übertragungsfehler oder defekten Geräten.

Angriffsziele von absichtlichen Störungen sind im grundsätzlich Hardware, Software und die Daten, wobei nicht vernetzte Systeme in der Regel weniger gefährdet sind, als vernetzte. Um eine höchstmögliche Netzwerksicherheit, genauer Kommunikationssicherheit, zu erreichen, wie dem Schutz vor Manipulationen und Abhören, hat die schon seit der Antike übliche Kryptographie in den letzten Jahrzehnten wesentliche Forschritte erzielt, und nahezu perfekte Konzepte entwickelt. Zusätzlich müssen rein technisch-organisatorische Konzepte vorgesehen werden, um Sicherheit vor Eindringlingen zu gewährleisten; hier leisten eine Art elektronischer Portier (Firewalls), elektronische Schlösser (Authentication Systems) als auch Alarmanlagen (Intrusion Detection Systems) wertvolle Dienste. In weiterer Folge erkennen und beseitigen elektronische Schnüffelprogramme die trotz der Sicherheitsvorkehrungen eingedrungenen Spezies, wie Viren, Trojanische Pferde oder Würmer.

Computerviren sind Programme, die sich selbst reproduzieren, indem sie sich an andere Programme anhängen. Sie brauchen also einen ausführbaren Wirt. Ein Wurm ist ein eigenständiges Programm, das sich selbständig übers Internet oder per Email wie ein Virus ausbreitet. Wie bei einer menschlichen Krankheit, treten deshalb vergleichbare krankhafte Symptome bei Computern auf. Häufig wird dagegen mit Selbstmedikation angekämpft, zum Beispiel Firewall Software einfach dem Anwender überlassen, die dann nicht den gewünschten Effekt erzielen kann. Genauso könnte man plakativ vergleichen, daß man einem Kranken auf dem OP das chirurgische Besteck reicht. Das Problem benötigt einen ganzheitlichen Lösungsansatz, denn der schlichte Einsatz einer Firewall und ziellose Installation von Schutzsoftware ist vom heutigen Stand der Technik einfach zu wenig – vielmehr führen präventive organisatorische Maßnahmen zu einer raschen Reduktion des Infektionsrisikos.

Trojanische Pferde sind im Gegensatz zu vielen Viren eigenständige Programme mit mehr oder weniger bösartigen Funktionen. Ihre schädigende Komponente ist in ein Programm eingebaut, das eine nützliche Funktion vortäuscht. Ein Trojaner gibt sich als Spiel oder anderes nützliches Tool aus, um im Hintergrund sein bösartiges Handwerk zu betreiben. Mit Hilfe eines Trojaners gelingt es, die vollständige Kontrolle über einen infizierten Rechner zu erhalten, was äußerst unangenehme Folgen für das oft ahnungslose Opfer haben kann.

Schutzziele vor diesem ungebetenen bösen Zoo, als auch vor Hackern und Crackern können wie folgt definiert werden:

- Vertraulichkeit: Nachrichteninhalte dürfen niemandem außer dem Kommunikationspartner bekannt werden Der Sender und Empfänger sollen die Möglichkeit haben, unbeobachtet und anonym zu kommunizieren
- Integrität: Fälschungen sollen erkannt werden

  Der Empfänger soll nachweisen können, daß eine Nachricht vom Sender, womöglich zu einem bestimmten Zeitpunkt, geschickt worden ist.

  Der Absender soll das Absenden einer Nachricht mit korrektem Inhalt, womöglich zu einem bestimmten Zeitpunkt, nachweisen können.
- Mehrseitige Sicherheit: Jeder wird gegen andere weitgehend geschützt

  Erfordernis des Einsatzes bestimmter Verfahren, die auch genutzt werden können

Für all die oben genannte Ziele bietet die Kryptographie interessante Lösungsmöglichkeiten. Das nachfolgende Schutzziel kann nicht mit deren Hilfe gelöst werden, sondern muß sowohl technisch-organisatorisch als auch mittels redundanten Back-up oder Stand-by Systemen erreicht werden.

- Verfügbarkeit: Zuverlässige Kommunikation zwischen allen Teilnehmern, die es wünschen, und denen es nicht verboten ist.

Die Folgen erfolgreich sabotierter Systeme können durchaus dramatisch ausfallen, wie zum Beispiel:

Ausspähen privater Daten oder Firmendaten, Verlust der Privatsphäre, Wettbewerbsnachteile, Fernsteuerung des Rechners, Mißbrauch des Rechners für kriminelle Zwecke im Namen des Opfers, Zerstörung oder Veränderung von Daten und Programmen, Kosten der Wiederherstellung, Haftungsfragen in Folge Regreßforderungen, Existenzbedrohung, strafrechtliche Verfolgung, ...

Um solchen Bedrohungsszenarien zu begegnen, müßte zu allererst die Büroinfrastruktur als auch benachbarte Systeme dokumentiert werden, um danach eine Risikoanalyse durchzuführen zu können. Danach wären geeignete Schutzmaßnahmen und Schutzpläne zu entwerfen, die in regelmäßigen Abständen auditiert und angepaßt werden.

Man muß sich jedoch bewußt sein, daß eine 100%-ige Sicherheit nie erreichbar ist. Letztendlich ist es ein betriebswirtschaftliches Kalkül, welchen Wert an Daten und Systemen man schützen muß, und in Relation dazu die Kosten die nötig sind aufstellt, um diese Daten und Systeme zu schützen.

4 DATENINTEGRITÄT

Gerade im Planungs- und Vermessungsbereich ist schon vor Jahrzehnten Pionierarbeit geleistet worden, was den Einsatz der Datenverarbeitung betrifft. Aus diesem Grund gibt es in diesem Bereich ein hohes Maß an Wissen, wie Daten über lange Zeiträume integer und dauerhaft gehalten werden können, aber auch das Bewußtsein für die Begleiterscheinungen solch, zwar einfach klingender, aber dennoch komplexer Anforderungen.

Fragen der Datensicherung und der Archivierung sind schon im vorherigen Kapitel der IT-Sicherheit eine Rolle gespielt, haben aber gerade hier eine zentrale Rolle. Als erstes fällt hier die Problematik des zu wählenden Mediums auf. Es ist nicht nur eine Frage, ob die Daten auf diesem Medium dauerhaft gespeichert, also auch in Zukunft fehlerfrei lesbar sind, sondern auch, ob in der Zukunft noch Geräte, Schnittstellen und Software verfügbar sein werden, die diese gespeicherten Daten lesen und korrekt interpretieren können. Es ist in diesem Zusammenhang ein berühmter Fall zu erwähnen, wo die Daten der Apollo-13 Mission weitgehend verloren sind. Aus diesem Grund kauft die NASA seit Jahren ausgediente Rechner und Medien auf, um dieser Problematik in der Zukunft rechtzeitig begegnen zu können. Eine Notwendigkeit in diesem Zusammenhang ist das Umkopieren und Umformatieren der gespeicherten Daten auf neue, dauerhafte, auch in der Zukunft absehbar unterstützte Medien und Geräte, da gerade im Planungs- und Vermessungsbereich die dreißigjährige Haftungsdauer für Bau-, Bestands- und Vermessungspläne als „Damoklesschwert“ über den Planungsbüros hängt. Diese Problematik erhält eine noch größere Tragweite, da die Daten immer mehr und vielfältiger werden.

In diesem Zusammenhang wäre auch kurz die Geschichte als Beispiel heranzuziehen, um diesem Thema eine allgemeine, schon seit Jahrtausenden, bestehende Wichtigkeit hervorzuheben. Viele antike Werke wären nie ohne die Kopierarbeit im arabischen Raum, als auch in den mittelalterlichen Klöstern, erhalten geblieben. Durch die Weitsichtigkeit der alten Ägypter, der Wahl von dauerhaften Speichermedien wie Stein und Papyrus, wird uns eine seit Jahrtausenden vergangene Epoche lebendig erhalten; und trotzdem ist genau hier die Problematik der Interpretation gespeicherter Daten aufgetreten, die inzwischen durch die Entzifferung der Hieroglyphen gelöst ist:

Die Datenformate stellen eine immer mehr komplexere Herausforderungen an das moderne Büro dar. Die zu speichernden Formate sind vielfältig, wie zum Beispiel für Textverarbeitung, Tabellenkalkulation, Plandaten, Bilddaten, Datenbanken, u.v.m. Diese Situation wird noch dadurch verschäft, daß sich die Versionen der eingesetzten Formate immer rascher ändern, mit der Folge, der Inkompatibilität, auch nur teilweise. Der schlimmste einzutretende Fall ist, wenn ein Datenformat nicht mehr lesbar wird, da ein Softwareprodukt nicht mehr unterstützt wird, oder dessen Hersteller nicht mehr existiert. Um dieser Herausforderung möglichst zu begegnen, sollte man sich folgende Anforderungskriterien an eine Software und dem Datenformat überlegen:

- Muß eine exakte oder möglichst authentische Reproduktion gewährleistet sein?

- Was ist der Zweck der Datenverarbeitung? Sind Vektor-, Raster- oder Textdaten zu verarbeiten?
- Wie ist die Politik und Liquidität des Herstellers? Ist eine möglichst langjährige Unterstützung absehbar?
- Existieren Import- und Exportschnittstellen zu anderen Anwendungen? Wie authentisch ist dann die Kopie?

An dieser Stelle kann man über die Sinnhaftigkeit proprietärer Formate von Softwareherstellern diskutieren, aber auch über die Zweckmäßigkeit von offenen Standards, wie XML und GML oder möglicherweise etablierter Formate wie Postscript. Auch für die Frage bestehender oder noch zu schaffender Normen wäre hier ein Platz. Weiters sind Fragen des Datenaustausches, der Wichtigkeit der Metadaten, und von Weiterverarbeitungsmöglichkeiten genau zu klären, bevor man sich auf Anwendungen und Datenformate festlegt.

Letztendlich ist der Erhalt der Datenintegrität, das heißt, die Erhaltung der Zugehörigkeit von Daten und deren Interpretierbarkeit, besonders bei Planungs- und Vermessungsbüros von besonderer Bedeutung. Würden zum Beispiel die Strichstärke von Plandaten bei Umwandlung in ein Rasterformaten verändert, oder bei der Speicherung mit verlustbehafteten Kompressionsverfahren ganze Flächen, wäre eine authentische Reproduktion des Originals anhand der Kopie unmöglich.

Letztendlich gilt es zu bedenken, daß beim Erstellen von Urkunden, auf das spätere Reproduzieren einer authentischen Kopie Bedacht genommen werden muß, auch im Zusammenhang einer 30-jährigen Aufbewahrungsdauer. Diese Aufgabenstellung wird den Büros nicht erspart bleiben, im Gegenteil, die elektronisierung von Urkundenarchiven schreitet in rasanten Schritten voran.

5 VERTRAULICHKEIT

Zum Schluß soll noch ein kurzer Einblick auf die Probleme, die im Zusammenhang mit der Vertraulichkeit der Daten stehen, hingewiesen werden. Auf der einen Seite wird dieser Schutz juristisch erreicht, wie zum Beispiel dem Datenschutzgesetz, Signaturgesetz oder dem Strafgesetzbuch. Bei Verstoß drohen dem Deliquenten Konsequenzen, wie Strafen. Auf der anderen Seite ist es auch technisch und organisatorisch möglich, sich vor unberechtigter Weitergabe und Ausspähen von Daten zu schützen; hier sei auf das Kapitel IT-Sicherheit verwiesen.

Computerkriminalität ist ein deliktisches Handeln, bei dem der Computer das Werkzeug oder das Ziel der Tat ist. „Deliktisch“ ist ein Begriff aus dem Strafgesetzbuch (StGB); damit meint man ein strafbares Handeln. Dabei kann der Computer das Werkzeug oder das Ziel sein, und zwar für Manipulation, Sabotage und Spionage.

In diesem Kapitel beschäftigen wir uns mit der Spionage. Trotz aller Gesetze und Strafbestimmungen ist es sinnvoll, sich vor Angriffen zu schützen; denn auch wenn man den Täter ausfindig macht, der Schaden läßt sich nur selten wieder gut machen. Bei Schadenersatzansprüchen wird oft ein Vergleich gesucht, um längere Prozesse zu vermeiden. Das bedeutet, daß der Geschädigte nur einen Teil des Schadens ersetzt bekommen wird. Ist trotzdem ein Vergleich nicht möglich, so ziehen sich solche Verfahren doch jahrelang hin, was zusätzlich einen bedeutenden Zeit und Kostenaufwand für den Geschädigten darstellt. Sich zu schützen hat auch einen weiteren Aspekt: Versicherungen halten sich gerne leistungsfrei bei Vorsatz und grober Fahrlässigkeit.

Einige Maßnahmen zur Erhöhung der Vertraulichkeit der Daten könnten so aussehen:

- Verschlüsselung der Daten, eventuell der Software und Freigabe mittels Schlüssel
- Authentifizierung der User und Paßworteinsatz
- Ein Paßwort muß regelmäßig geändert werden, und absolut geheim bleiben
- Vorsicht vor Erspähung von Paßworten
- Kathodenstrahlröhren (Cathode Ray Tube, CRT), Geräte und Kupferkabel erzeugen eine Strahlung die mittels speziellen Geräten empfangen werden kann, wobei der z.B. dargestellte Bildschirminhalt dann sichtbar wird.
- Überprüfung des Programmcodes eines Programmierers durch andere Programmierer
- Vernichten nicht mehr benötigter Festplatten, Disketten oder Ausdrucken (Mistkübel sind oft eine interessante Informationsquelle)

Ein letzter Aspekt: all diese Maßnahmen sind wirkungslos, wenn der Spion im eigenen Unternehmen steckt; Untersuchungen haben ergeben, daß die meisten Angriffe von eigenen zugangsberechtigten Mitarbeitern durchgeführt werden, oder daß Geheimnisse von diesen nach außen getragen werden. Umso wichtiger ist es Maßnahmen zu setzen, damit Zugangsberechtigte zu sensiblen Daten erst gar nicht in Versuchung geraten, solche Handlungen zu setzen; das wären zum Beispiel Mitarbeiterzufriedenheit, Gehalt, Kontrolle, Strafandrohungen, Aufklärung, u.v.m.