Computerkriminalität

Ganzheitliche Sicherheit im Unternehmen

Hacker und Sicherheitsbeauftragte liefern sich einen immer schneller werdenden Wettlauf. Welche Handlungsalternativen haben Entscheider in Unternehmen für die Implementierung von Sicherheit?

Es besteht die Möglichkeit, zunächst einmal alles so zu belassen, wie es ist: Warum etwas ändern, wenn für ein akzeptables Restrisiko sicherstellende Maßnahmen etabliert sind?

Historisch/pragmatischer Ansatz	Strategischer Ansatz
• Bottom-up • Fokus auf Infrastruktur, Systeme und Anwendungen • IT-Sicherheitsstandards i.d.R. vernachlässigt • Lückenhaftes/inkongruentes Sicherheitsniveau	• Top-down • Geschäftsprozess-bezogen • Bewertung von Prozessen und Daten • Implementierung von Sicherheit auf allen Ebenen • Basierend auf Standards • Wirtschaftlicher?

Trotzdem verlangen Gesetze heute aus gutem Grund, im Bereich des Risikomanagements proaktiv zu sein. Schlagworte wie Frühwarnsystem, Internes Kontrollsystem, Corporate Governance stehen im Raum.

Klassischer pragmatischer vs. strategischer Sicherheitsansatz

IT-Sicherheit wurde im wesentlichen durch auf Erfahrung beruhendem pragmatischem Vorgehen konzipiert und implementiert. Es wurden ausschließlich Anwendungen, Systeme und Netze betrachtet und bestenfalls noch infrastrukturelle Aspekte berücksichtigt. Die Organisation des Unternehmens und seine Geschäftsprozesse wurden meist nicht betrachtet.

Durch die pragmatische Vorgehensweise besteht die Gefahr, Sicherheit für nachrangige Prozesse zu implementieren und generelle IT-Sicherheitsstandards zu vernachlässigen. Die Konsequenz ist ein inkongruentes, Lücken öffnendes Sicherheitsniveau.

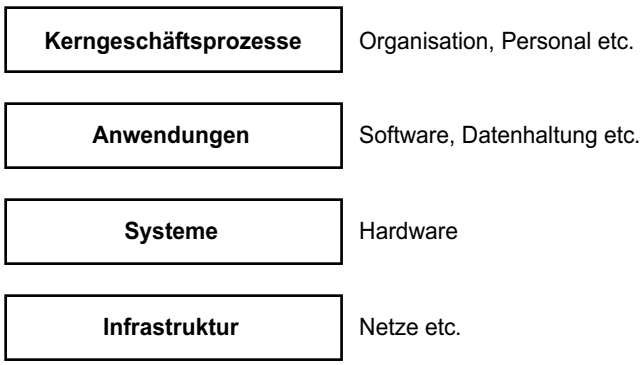
Durch den strategischen Ansatz kann ein lückenhaftes und damit unwirksames Sicherheitssystem vermieden werden: Top-down werden Geschäftsprozesse, Anwendungen, Systeme und dann IT-Sicherheitsmaßnahmen dokumentiert, konzipiert und implementiert. Bereits im Rahmen der Prozessanalyse werden Weichen für Sicherheits-Implementierungen gestellt.

Strategisch ausgerichtete Vorgehensweise

Ein strategischer Ansatz nutzt als oberste Leitlinie das von der betreffenden Unternehmung betriebene Geschäft. Ausgangspunkt aller Analysen ist die Betrachtung der betrieblichen Kernprozesse.

Zur Analyse der betrieblichen Risikolage eignen sich die von den Big Five zur Abschlussprüfung und Beratung eingesetzten Business Risk Models gut: Zunächst werden die Geschäftsprozesse der Unternehmung dokumentiert und bewertet. Dabei werden Umfeldrisiken (Konkurrenten, Marktlage etc.) genauso in Betrachtungen einbezogen wie prozessinhärente Aspekte (interne Organisation, Personal etc.). Diese schon recht detaillierten Untersuchungen liefern ein genaues Bild der Kerngeschäftsprozesse einschließlich vorhandener Abhängigkeiten.

Von den Dateneigentümern wird der Schutzbedarf des Datenbestandes erhoben. Dies entscheidet über die Bedeutung der Daten für das Unternehmen. Dieser Prozess betrachtet nicht allein die zu verarbeitenden und zu

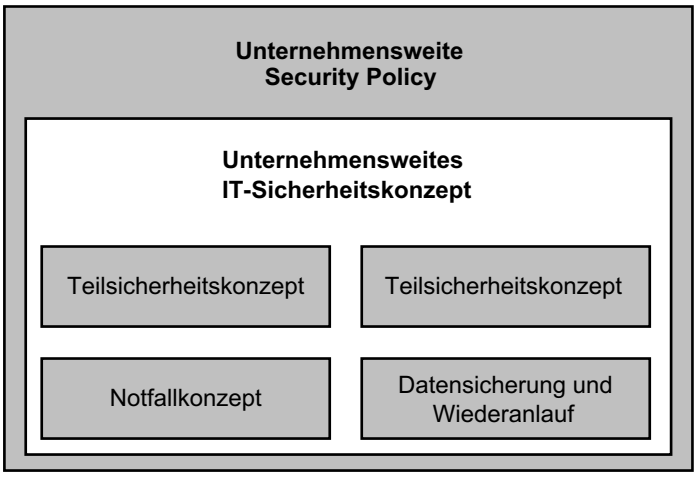


übertragenden Daten, sondern berücksichtigt darüber hinaus die betreffenden Anwendungen und Systeme.

Hilfestellung bei der Priorisierung leisten Bedrohungsszenarien, nicht wie beim klassisch-pragmatischen Ansatz einzelne Bedrohungen. Diese integrierte Vorgehensweise soll Maßnahmen ausschließen, die gegen immaterielle Einzelbedrohungen gerichtet sind. Die Anwendung von Bedrohungsszenarien ermöglicht darüber hinaus eine realitätsgetreue, besser auf Unternehmensziele ausgerichtete Risikobetrachtung.

Umsetzung eines strategischen IT-Sicherheitsansatzes

Wie sieht die Dokumentenstruktur eines strategischen IT-Sicherheitskonzeptes aus? Ausgangspunkt ist eine Security Policy, welche die unternehmensweite IT-Sicherheitspolitik auf einem hohen Abstraktionsniveau beschreibt. Darauf bauen IT-Sicherheitskonzepte oder Teilkonzepte (z.B. ein Firewall-Konzept) auf. Es folgen Organisationsanweisungen, Prozessbeschreibungen, Sicherheitsempfehlungen etc. Die folgende Grafik verdeutlicht eine solche Struktur:



Die technische Umsetzung von strategischen Maßnahmen umfasst sowohl globale als auch spezifische Maßnahmengebiete. Es ist nicht mehr vorgesehen, einzelne Systeme bzw. Systemgruppen abzusichern, sondern alle Maßnahmen sind Teil einer unternehmensweiten Sicherheitsstrategie, die aufeinander abgestimmt ist. Daraus ergeben sich wirtschaftliche Vorteile, da Synergieeffekte genutzt werden können und durch geschäftsprozessbezogene Maßnahmen kritische Situationen für die IT-Sicherheit vermieden werden.

Ein technisches Szenario kann z.B. auf einem zentralen Sicherheits-Server beruhen, der sowohl die Anmeldung der Nutzer mittels “Single-Sign-On” als auch die Kommunikation mit Anwendungs- und Fileservern für deren Rechteverwaltung übernimmt. Dabei meldet sich der User – abgesichert durch PKI und Smartcard oder biometrische Verfahren – nur noch einmal an; die Anwendungen tauschen dann mit dem Sicherheitsserver zur Authentisierung ein “Secondary Passwort” aus. Damit erhält man eine praktikable Lösung für das leidige Thema Passwort-Handling, bei dem der Spagat zwischen Benutzerfreundlichkeit und Sicherheit versucht werden muss.
Der Kommunikationsverkehr im Unternehmensnetz sollte ebenfalls verschlüsselt werden, um Daten- und Benutzerauthentifizierung sicherzustellen. Netzverkehr kann dann zwar abgehört werden, aber Informationen können daraus nicht mehr gewonnen werden. Für Banken wird diese Verschlüsselung der internen Kommunikation bereits vom Bundesaufsichtsamt für das Kreditwesen empfohlen.

Für die Abbildung der geschilderten Strukturen wird eine geeignete Middleware-Architektur benötigt, z.B. nach dem CORBA- (Common Request Broker Architecture) Standard.

Chancen und Risiken

Vorteil der strategischen Vorgehensweise ist die integrierte Realisierung unternehmensweiter IT-Sicherheitsmaßnahmen und das Vermeiden proprietärer Lösungen, die sich nicht ins Unternehmenskonzept einpassen und einen hohen Wartungs- und Supportaufwand erfordern. Risiken ergeben sich durch die hohe Komplexität von strategischen Sicherheitsprojekten, die durch die Knappheit von geeigneten Fachkräften oft außer Kontrolle gerät.

Bei allen Risiken überwiegen die Vorteile des beschriebenen Vorgehens deutlich. Es wird bei konsequenter Anwendung wirtschaftlich ein Höchstmaß an Sicherheit erreicht.

Frank Wissing, Stuttgart/Ludwigsburg

Résumé: une approche globale de la sécurité dans l'entreprise

Les entreprises sont aujourd'hui contraintes par différentes lois d'être actives dans le domaine de gestion des risques et de la sécurité. L'approche doit cependant changer: la démarche pragmatique bottom-up doit laisser la place à une démarche top-down qui prend en compte l'ensemble des processus et intègre la gestion des risques dans le design des processus.

Dans une telle démarche ce ne sont plus les risques isolés mais des scénarios de risques qui orientent la gestion de l'entreprise. Ces scénarios couvrent aussi bien les risques liés à l'environnement de l'entreprise que les risques internes.

Le tout repose sur une politique globale de sécurité fixée à l'échelon de l'entreprise, qui englobe les sous-concepts et garantit l'interopérabilité de ceux-ci. Une approche qui devrait éviter que les différents maillons de la chaîne soient trop disparates et assurer la mise en place d'une solution économique et exploitant au mieux les synergies entre les différents processus.

Computerkriminalität

Veruntreuungsfall bei der Zentralen Ausgleichsstelle (AHV/IV) in Genf

Dank der Aufmerksamkeit von zwei Mitarbeiterinnen wurde im September 1996 bei der Sektion IV-AHV/Sachleistungen ein Unterschlagungsfall aufgedeckt. Bei den Untersuchungen des internen Inspektorates der ZAS wurde festgestellt, dass der damals für diesen Bereich verantwortliche Sektionschef betrügerische Handlungen vollzogen hatte. In den Jahren 1994 bis 1996 hatte sich der Beamte in 57 Fällen Zahlungen im Gesamtbetrag von rund 115 000 Franken zu Lasten der IV an die Adresse seiner Mutter und den Hauswart seines Wohndomizils überweisen lassen. Zu diesem Zweck benützte er die Eingangsnummern von EDV-mässig erfassten, noch nicht zur Zahlung freigegebenen Lieferantenrechnungen und erstellte damit fiktive Rechnungen. Unter Zuhilfenahme der AHV-Nr. seiner Halbschwester und weiterer EDV-Manipulationen stellte er die Abstimmung mit den durch die IV-Stellen ausgestellten Verfügungen her. Die Zahlungsfreigabe aller IV-Sachleistungen erfolgte durch ihn selbst.

Die Hauptgründe, welche diese Veruntreuung ermöglichten, waren:

- Fehlende Funktionstrennung resp. Funktionskumulation des Delinquenten;
- Sein uneingeschränkter Zugriff und die umfassenden Kenntnisse des Informatiksystems;
- Blindes Vertrauen seitens der Vorgesetzten und Mitarbeiter in die Person des Sektionschefs, vorab wegen seines grossen Engagements in seinem Aufgabenbereich und für die Organisationseinheit;
- Fehlende Überwachungs-/Kontrollmassnahmen, v.a. aufgrund der Priorisierung der Erledigung des grossen Arbeitsanfalls und Aufarbeitung resp. Beseitigung von Rückständen bei den Auszahlungen.

In Absprache mit der Bundesanwaltschaft wurde der Betrugsfall der Strafverfolgungsbehörde des Kantons Genf übergeben, welche den Beamten mit Urteil vom 26. Juni 1997 wegen Betrugs und betrügerischem Missbrauch einer Datenverarbeitungsanlage zu zwölf Monaten Gefängnis bedingt mit einer vierjährigen Bewährungsprobe verurteilte. Der Beklagte wurde ausserdem zur Rückzahlung der gesamten Schadenssumme verpflichtet.

Computerkriminalität

Computerspuk im Erfassungssaal

Ein wahres Melodrama in fünf Akten

Übersetzt und adaptiert durch die Redaktion.

Personen und ihre Funktionen

- Kurt, Geschäftsführer einer Dienstleistungsgesellschaft
- Fritz, unabhängiger Informatikberater
- Lothar, Systemoperator der Dienstleistungsgesellschaft
- Peter, Klaus, Hans, Sepp, Computerprogrammierer des Softwarelieferanten
- Paul, Projektleiter des Softwarelieferanten
- Bettina, Sekretärin von Kurt
- Ada, Berta, Gertrud, Hanni, Maya, Petra, Zoe, Datenerfasserinnen der Dienstleistungsgesellschaft
- Tanya, Aushilfskraft

1. Akt: Der Programm- und Datenbankfehler

Kurt, Fritz und Paul sitzen in Kurts Büro am Konferenztisch. Kurts Dienstleistungsfirma, welche ein System von Pauls Softwarefirma zur Fakturierung und Buchhaltung für Dritte einsetzt, gerät zeitlich in der Verarbeitung stark in Verzug. Die Überstunden häufen sich, die Fehlerquote steigt ins Unerträgliche.

“Meine Herren, so kann es nicht weitergehen,” meint Kurt. “Wir geraten mit unserer Verarbeitung der Daten zeitlich mehr und mehr ins Hintertreffen. Meine Kunden sind nicht weiter gewillt, diese Verzögerungen zu akzeptieren. Es muss etwas geschehen. Allmählich hilft nicht einmal mehr eine Konventionalstrafe. Ich warte auf Vorschläge. Schliesslich sind *Sie* es, die uns dieses System empfahlen und schrieben.”

Er murmelt dann noch „alea jacta est“ hinzu, weil er in seiner Jugend zu viele Asterixbücher gelesen hatte und eine Vorliebe für römische Kaiser hegt.

Fritz windet sich in seinem Stuhl. “Moment. Ich habe mit der Entwicklung des Systems nichts zu tun. Ich kam erst dazu, als das Chaos schon im Gange war. Meiner Meinung nach ist das Design verknorzt und die Datenbank wird nicht optimal eingesetzt, woraus sich die langen Antwortzeiten ergeben. Kein Wunder, sind die Mädchen der Datenerfassung frustriert. Ob es überhaupt die richtige Datenbank für die Lösung der Problemstellung ist, weiss ich im Moment selber nicht. Eine Vorstudie, welche diesen Namen verdient hätte, gab es ja nicht.”

Paul kontert: “Eine Vorstudie gab es sehr wohl. *Oracle* ist eine gute Datenbank, die auf VAX mehrfach erprobt und erfolgreich eingesetzt ist. Peter ist ausserdem ein erfahrener Chefprogrammierer, dem eine Fahrlässigkeit sicher nicht angedichtet werden darf. Hans, Sepp und Klaus stehen unter seiner Aufsicht und sind ebenfalls gewiefte und hervorragende Programmierer. Es sind vielmehr diese unnötig eingesetzten Routinen, die angeblich zur Überwachung des Systems eingebaut wurden, welche die Verarbeitung verzögern.”

Fritz weist darauf hin, dass die *Audit-Routinen* auf Veranlassung von Peter in der Zwischenzeit entfernt worden waren. Um die Erfassung weiter zu beschleunigen, hatte Peter die Möglichkeit eingebaut, dass mehrere Leute gleichzeitig den gleichen Auftrag bearbeiten konnten. Damit wurden viele der zeitraubenden *Inserts* in der Datenbankverarbeitung eliminiert. Entsprechende, somit fehlende, Plausibilitätskontrollen waren auf Fritzens Verlangen aus der On-line-Erfassung in die Über-Nacht-Batch-Programme übertragen worden. Dies alles führte zu einer gewissen Beschleunigung der Verarbeitung. Allerdings genügte dies offenbar nicht.

Neu hinzugekommen war die Tatsache, dass sich die Fehlerquote bei der Massenerfassung in unangenehmer Art und Weise laufend erhöhte: Die Datenerfasserinnen standen offenbar derart unter Stress und Nervosität, dass sie verschiedene Fehleingaben tätigten und Flüchtigkeitsfehler begingen. Diese wurden dann in den Batchläufen entdeckt. Das Korrekturprozedere war zwar ziemlich effizient, aber doch zeitaufwendig.

Paul wirft die Frage auf, ob eine Erweiterung der Hardware und zusätzliche Arbeitsplätze in Erwägung gezogen werden. Fritz tut dies mit der Bemerkung ab: “Sie wollen ja nur weiter verkaufen und Kommissionen garnieren.”

Auch Kurt wehrt sich gegen eine zusätzliche Investition, weil der Kreditrahmen schon zweimal erhöht und gesprengt worden war. Mitten im Gespräch meldet sich Bettina via Intercom: “Herr Lothar ist hier und möchte Sie dringend sprechen.”

Unwillig schaut Kurt auf und meint: “Ich bin jetzt in einer Sitzung. Ich rufe später zurück.”

Als Bettina insistiert, dass es wirklich dringend sei, weil Herr Lothar melde, es sitze ein Virus im Computer, springen alle drei auf und reden durcheinander.

“Wie, was?!”
“Auch das noch!”
“Das kann natürlich auch ein Grund sein.”
“Von einem Virus auf einer VAX habe ich noch nie etwas gehört.”
“Das darf doch nicht wahr sein!”
“Wie so etwas?”
“Er soll hereinkommen.”
“Seit wann überhaupt?”
“So ein Mist.”
“Jetzt ist dann aber das Fass voll.”
“Uns kann doch so etwas gar nicht passieren.”
“Wer hat ihn denn eingeschleppt?”
“Wie heisst der Virus?”

Nachdem sich der Tumult etwas legt, versucht Kurt ruhiges Blut zu bewahren und zur Sachlichkeit zurückzukehren. “Wir haben es offenbar mit einer schwierigen Situation zu tun. Legen wir einmal alle Fakten auf den Tisch. Erstens: Herr Lothar, erklären Sie uns, weshalb Sie auf die Idee kommen, es sässe ein Virus im Computersystem!”

Es war folgendes geschehen: Wie jedes Monatsende war wieder einmal Feuer im Dach. Ausserdem war noch Vollmond. Alle Datatypistinnen arbeiteten wie wild. Gertrud stellte beim nochmaligen Durchlesen der soeben eingegebenen Daten fest, dass ein Teil in magischer Art und Weise verschwunden war. Es handelte sich in erster Linie um Namen neuer Kunden. Gertrud ärgerte sich, da sie annahm, sie hätte einen Eingabefehler gemacht und die Abweisungsmeldung des Systems übersehen. Beim zweiten Mal schaute sie sich scheu um, ob jemand ihre Fehlleistung beobachtet hätte. Beim dritten Mal schossen ihr vor Wut die Tränen in die Augen. Sie holte Lothar und zeigte ihm die Bescherung.

“Bist Du auch sicher, dass Du die Daten eingegeben hast?”
“Also den Namen Bodenmüller habe ich nun dreimal eingegeben, das weiss ich genau. Ich bin doch nicht blöd.”

Die andern Datatypistinnen hatten aufgehört zu arbeiten und schauten zu. Hanni und Ada kamen herbeigeeilt, um den Sachverhalt zu verifizieren. Tatsächlich fehlte eine ganze Reihe von Namen der eingegebenen (aber vom System noch nicht verarbeiteten) Daten. Genau dies war bei der festgestellten Fehlerhäufung offenbar auch passiert. Da dies aber nicht nur Gertrud, sondern alle Datatypistinnen betraf, war die Erscheinung mit der allgemeinen Nervosität abgetan worden.

Hier konnte aber kein Zufall mehr vorliegen. Auch war die Fehlerrate solchen Ausmasses bei der sonst zuverlässigen Gertrud nicht denkbar. Unter Aufsicht aller Augen korrigierte Gertrud die Fehler, um den Batch dann ordnungsgemäss abzuschliessen. Alle atmeten auf. Der Namenfresser war verschwunden.

Alle kehrten an ihre Arbeit zurück und arbeiteten nun umso fleissiger, weil ja bei der Aufregung über eine Viertelstunde verloren gegangen war. Auf Gertrud wartete allerdings eine ungemütliche Überraschung. Nach einiger Zeit trat der Namensfresser wieder auf, worauf sie unverzüglich Lothar alarmierte.

“Wahrscheinlich bin ich einfach hysterisch,” kicherte Gertrud. Hanni tröstete: “Für Hysterie haben wir nun wirklich keine Zeit.” Berta pflichtete bei: “Hier sollte jemand eingreifen.”

Das war dann der Moment, als Lothar beschloss, in die Sitzung zu platzen.

Fritz übernimmt das Kommando. Nachdem die verschiedenen Sachverhalte registriert sind, schliesst er scharfsinnig auf einen Datenbank- oder Programmierfehler, der wahrscheinlich auf das gleichzeitige Bearbeiten von Aufträgen zurückzuführen ist. Paul übernimmt zähneknirschend den Auftrag, alle Routinen mit Peter und andern Programmierern des Softwarelieferanten über das nahe Wochenende in dieser Hinsicht zu überprüfen.

Mit bemerkenswerter Akribie sucht, kontrolliert, simuliert und prüft Paul mit seinen Mitarbeitern über das ganze Wochenende. Ergebnis: Leermeldung. Seufzend gibt Paul schliesslich zu, keinen Fehler gefunden zu haben. Möglicherweise liegt der Fehler beim Hersteller der Datenbank. Fritz übernimmt es, bei *Oracle* nachzufragen, ob einschlägige Fälle dort bekannt sind, und wie ihnen begegnet wurde.

Die Empörung bei *Oracle* ist gross: Eine schamlose und geschäftsschädigende Unterstellung. Fritz bohrt und erwähnt einen Fall aus seiner Praxis, bei welchem tatsächlich in einer bestimmten Version einmal ein Fehler durch die Kontrollmaschen der Datenbanksoftware geschlüpft war. Der Sachbearbeiter wird stiller und vorsichtiger. Er verspricht zurückzurufen. Er erkundigt sich noch nach der Belastung des Systems.

Fehler in der Datenbanksoftware? Nein. Die Abklärungen ergeben, dass Fritz zwar recht hatte, jene Version jedoch vor etlicher Zeit nur kurz bei wenigen Kunden eingesetzt worden war, aber sicher nicht bei Kurts Dienstleistungsgesellschaft.

2. Akt: Das Virus

Nach dem Wochenende tritt der "Datenbankfehler" nicht mehr auf. Er ist verschwunden. Als zwei Tage später Petra krank wird und Zoe gleichzeitig in den Ferien weilt, stellt sich erneut Stress in der Datenerfassung ein. Prompt tritt auch der Störenfried wieder auf. Er frisst diesmal nicht ganze Namen, sondern nur jeden zweiten Buchstaben. Maya entdeckt dies als erste, und ihr stockt der Atem.

Fritz tritt wieder auf den Plan. Er kennt ein Mittel gegen den Unhold: Er lässt die *delete* Möglichkeit sperren. Sollte ein solcher nötig sein, musst immer Peter eingreifen. Dies ist zwar lästig, aber tatsächlich, der Buchstabenfresser verschwindet.

Fritz ist triumphierend der Ansicht, Paul hätte mit seiner Crew eben nicht richtig gesucht. Es sei eben doch ein Datenbank- bzw. Programmfehler. Da erscheint Gertrud und verkündet, dass ihre Namen neuerdins mit Sonderzeichen wie %, ç, {, usw. entstellt würden. Jetzt ist auch Fritz überzeugt: Es sitzt ein Virus im System. Als die Verstümmelungen sich noch in *olé!* und *hihihi* wandeln, ist klar, dass Unfug im Spiel ist. Von einem Datenbankfehler kann keine Rede sein.

"Uff." Peter und Paul atmen vorerst einmal halbwegs erleichtert auf. Der Fehler ist doch nicht bei ihnen.

Fritz geht über die Bücher. Wie soll man das Virus entdecken? Welches sind die Erscheinungsformen? Fritz setzt sich neben Gertrud, Ada, Berta, Hanni, Petra und die Aushilfskraft Tanya. Hier schlägt das Virus denn auch das nächstemal zu: Das Batchtotal veränderte sich offenbar unbemerkt während der Erfassung, so dass die Buchungsmappe nicht abgeschlossen werden kann. Fritz reibt sich die Augen. Das darf doch nicht wahr sein.

Die inzwischen genesene Petra meldet, dass eine Rechnung verschwunden sei, die sie schon vier Mal eingegeben habe. Fritz hatte gar nicht gewusst, dass er so viele unanständige Wörter kannte, wie er jetzt gerade braucht. Unter aller Augen korrigiert die hilfsbereite Hanni erfolgreich den Batch.

Hartnäckig lässt Fritz sodann weiter erfassen und sagt sich innerlich, "einmal erwische ich Dich schon, Du "+%!*Q".

Gegen Mittag scheint das Virus müde zu werden, um in der Mittagspause die Aktivität ganz einzustellen. Aber am Nachmittag kehrt seine Vitalität zurück, obschon Fritz auch Peter als Überwacher einsetzt. Gegen vier Uhr verschwindet das Virus. Die Datatypistinnen gehen um sechs Uhr erschöpft und entnervt nach Hause. Ziemlich zerstört sitzen Peter, Fritz und Lothar zusammen. Zermürbt gestehen sie dem händeringenden Kurt, dass ihr Suchen bisher erfolglos geblieben ist. Dieser verwünscht die römischen Kaiser und zitiert Jesaja 6,11: "Wie lange, oh Herr?" Das Verhalten des Virus' war derart unstet und irreal, dass bei Fritz der Verdacht wächst, es sei ein Hacker am Werk.

3. Akt: Der Hacker

Für diese Theorie spricht, so meint Fritz, dass das System offen ist: Wählleitungen und eine X.25-Verbindung, um *remote.maintenance* von Pauls Büro aus betreiben zu können. Gegen die Theorie spricht, dass niemand aus dem Unfug Gewinn zieht: Die einmal vom System akzeptierten Daten werden nicht mehr angetastet; Gelder werden keine abgezweigt, ausgetretene unzufriedene Angestellte (die das nötige Know-how hätten) sind nicht bekannt, die Programmierer arbeiten infolge Terminüberschreitung seit Wochen gratis. Es ist also keine Bereicherung erkennbar.

Dennoch besteht Fritz darauf, dass die Verbindungen abgeschaltet werden. Päng! Der Ungeist ist verschwunden!

Triumphierend lässt Fritz eine spezielle Abfangroutine schreiben, um die via Telefonnetz empfangenen Meldungen besonders genau zu untersuchen, bevor sie ins System gelassen werden. "Fingerabdruck mit Kennung, Uhrzeit und Before/Afterimage" tauft Fritz

seine Erfindung und führt sie stolz Kurt vor. Gerade will er das erste Modem aktivieren, als das Virus bei Gertrud wieder zuschlägt: Ein Batch wurde verstümmelt. Also doch ein Virus? Kein Hacker? Oder beide zusammen? Womöglich noch ein Programmfehler dazu? Es ist zum Verzweifeln. Kurts Aspirinpegel hat ärztlich verbotene Höhen erreicht.

4. Akt: Höhepunkt und Katharsis

Praktisch am Ende der Kräfte fragt sich Fritz nach Tagen erfolglosen Suchens nicht mehr, welcher Art der Unhold ist, sondern nur noch, wie er ihn umbringen soll. Lothar, Fritz und Peter einigen sich darauf, den *Audit-Trail* von *Oracle DBMS* wieder in Kraft zu setzen. Zudem werden alle Bevor- and After-Images in einer separaten Tabelle abgespeichert und lückenlos untersucht: Laufend aufgenommene Fingerabdrücke, sozusagen.

Ein paar Tage passiert nichts. Dann, aus heiterem Himmel: Schnapp, die Falle ist zu. Drin sitzt … wer wohl? … Zoe!

Aber das ist doch gar nicht möglich! Zoe ist auf einer Trauminsel ohne Telefon in den Ferien und gar nicht anwesend! Zudem ist die Verbindung nach aussen gerade abgeschaltet. Irgend jemand muss mit Zoes Identifikation Unfug treiben. Telepathie? Telekinese? Fritz ist allmählich nicht einmal mehr sicher, ob er Fritz heisst.

Apathisch setzt er sich zu Gertrud an das Erfassungsgerät, um seine Beobachtungen am "lebenden Objekt" weiterzuführen. Das System ist gerade etwas weniger belastet, weil Tanya das irre Geisterhaus fluchtartig verlassen hat, Petra auf der Toilette die Nase pudert und Maya einen Apfel isst.

"Wuff" erscheint auf Getruds Bildschirm. Wie von der Tarantel gestochen fährt Fritz auf und stürzt sich nicht auf Getruds Bildschirm, sondern auf jenen der wenige Schritte entfernt ruhig arbeitenden Hanni. Sie ist auch unter "Gertrud" eingeloggt und tippt gerade ohne eine Miene zu verziehen "Yuppie" ein. Fritz trifft der Schlag. Ausgerechnet die hilfsbereite Hanni!

Verlegenheit. Empörung. Fristlose Entlassung.

Warum? Niemand weiss es. Hanni bringt keine Erklärung vor. Es ist weder Rache noch Unzufriedenheit. Geschickt worden war sie auch nicht, um Sabotage zu betreiben. Zufällig hatte sie entdeckt, dass sie mit einer Identifikation einer andern Person gleichzeitig im System tätig sein und somit spielen konnte. Später erfuhr sie in der Kaffeepause und beim Mittagessen weitere Identifikationen und Passwörter, so dass sie nicht nur mit der Erstgeschädigten (Gertrud), sondern mit allen andern auch ihren Spass haben konnte.

Sucht? Eine Art Pyromanin? Bis heute bleibt das Rätsel ungelöst – Hanni ist verschwunden und gilt heute als verschollen. Allen ist es recht, ausser Gertrud. Sie hätte Hanni noch eine Chance gegeben.

Die Identifikationen und Passwörter waren übrigens Hanni bekannt gegeben worden, weil sie sich so hilfreich beim Beheben der Fehler einsetzte. Verdacht schöpfte niemand. Fritz weiss auch heute noch nicht, warum er sich in jenem kritischen Moment auf den Bildschirm von Hanni gestürzt hatte.

5. Akt: Epilog oder die Moral von der Geschichte

Ein sich am Kopf kratzender Kurt (der eine unerfreuliche fristlose Entlassung hatte aussprechen müssen), ein übermüdeter Peter sowie ein nervöser Paul sitzen wieder in Kurts Büro.

"Diem perdidi." Kurt hat zu Asterix bzw. Titus zurückgefunden.
"Gar nichts ist verloren," wehrt sich der des Lateinischen halbwegs mächtige Fritz. "Wir müssen die Lehren aus dieser Geschichte ziehen und interessierten Kreisen zur Verfügung stellen."

Die "Detektive" kommen zu folgenden Schlüssen:

Sicherheitsbewusstsein

Dies ist wohl *der* Eckstein. Auch wenn keine unmittelbare finanzielle Versuchung vorliegt, muss das Sicherheitsdenken des Personals gefördert werden. Bei Kurts Dienstleistungsfirma war dieser Punkt vernachlässigt worden. "Wir haben doch diese Kleinkariertheit nicht nötig," wurde immer wieder grosszügig verkündet. "Ausserdem besteht bei uns gar kein Anreiz, ein Passwort unnötigerweise zu kennen." „Bei uns könnte man geradeso gut ohne Passwort arbeiten." Hochmut kommt bekanntlich vor dem Fall.

Das Sicherheitsbewusstsein muss mit ausbildungsbezogenen, disziplinarischen und technischen Mitteln unterstützt werden.

Geheimhaltung des Passwortes

In Kurts Firma waren Passwörter freiwillig an Mitarbeiter(innen) weitergeben worden. Es trifft zu, dass Systeme gebaut werden, um benützt zu werden (und nicht, um deren Benützung zu verhindern). Passwörter sind aber ein anvertrautes Gut, welches mit Sorgfalt zu behandeln ist. Wird es weitergegeben, verliert es seinen ursprünglichen Sinn und Wert.

Mitarbeiter sollten bei ihrer Einstellung eine schriftliche Erklärung abgeben, dass sie davon Kenntnis genommen haben, dass Passwörter nicht verraten oder weitergegeben werden dürfen. Verletzungen dieses Grundsatzes sind unnachsichtig zu ahnden.

Beachten der Systemmeldungen

Das Betriebssystem VAX-VMS meldet, wann der betreffende Sign-On letztmals verwendet wurde sowie die Anzahl erfolgloser Sign-On-Versuche der betreffenden Kennung. Diese Meldungen wurden bei Kurt überhaupt nicht beachtet. Hätte z.B. Petra nach ihrer krankheitsbedingten Abwesenheit gemeldet, dass jemand offenbar in ihrer Abwesenheit ihre Kennung mit Passwort benutzt hatte, wäre Fritz wahrscheinlich schneller auf die Ursache der unheimlichen Erscheinung gestossen.

Mitarbeiter sind auf die Möglichkeit einer Hackertätigkeit hinzuweisen. Systemmeldungen bezüglich der Verwendung von Kennungen sind zu beachten.

Vergabe neuer Passwörter

Gewisse Systeme (wie z.B. VAX-VMS) bedingen, dass der Systemverantwortliche bzw. der Security Officer das Passwort setzt. Die Bekanntgabe an den Benutzer sollte allerdings nicht leicht hörbar (Lothar hatte es jeweils der betreffenden Person laut zugerufen!) erfolgen. Auch in Ausnahmefällen und in Eile ist die Geheimhaltung zu beachten.

Neue Benutzer

Bei Kurt war das Einrichten neuer Benutzer etwas umständlich und benötigte in den meisten Fällen die Hilfe eines Programmierers. Lothar hatte deshalb aus Bequemlichkeitsgründen für die temporär anwesende Tanya die Identifikation der einmal früher bei Kurt tätigen Flora reaktiviert.

Das Einrichten neuer Benutzer ist für den Systembetreuer einfach zu gestalten. Die Tätigkeit des Security Officer sollte auch durch eine Person wahrgenommen werden können, die nicht Systemprogrammierer ist.

Gestaltung der Passwörter

Bei Kurt waren die Regeln, wie sie in der Fachliteratur nachzulesen ist eingehalten: Mindestens sechs Zeichen, zufällig vermischte Buchstaben, Ziffern und Spezialzeichen. Trotzdem war der Fall passiert. Vielleicht auch gerade deshalb. Für den einfachen "Mann auf der Strasse" sind wilde Zeichenkombinationen schwer zu memorisieren.

Passwörter sollten im Kopf behalten werden können. Sie dürfen aber auch nicht zu einfach sein, so dass sie leicht erraten werden könnten. Sie sind häufig zu wechseln. Die gegebenen Systemunterstützungen zum Zwang des Passwortwechsels sind auszunützen.

Multiple Logins

Der Doppelgänger führte die Spezialisten an der Nase herum. Der Druck der Effizienzsteigerung hatte zu einer sträflichen Vernachlässigung der Sicherheit geführt. Auch der nachträglich vorgebrachte Rechtfertigungsversuch, die Massnahme sei auch für Stellvertretungen elegant, greift nicht.

Kein Sign-On darf in einem System gleichzeitig mehr als einmal aktiv sein.

Audit Trail der Anwendung

Die Anwendung hielt bei jeder Transaktion fest, welcher Benutzer zuletzt an einem bestimmten Datensatz gearbeitet hatte. Allerdings fehlten die Angaben bezüglich Zeit und Änderungsinhalt.

Der Prüfpfad ist nur einwandfrei und lupenrein, wenn bei Änderungen von Daten sowohl Ausführender, Datum und Zeit, als auch Inhalt (before/after) festgehalten wird.

"Quod erat demonstrandum," meinte Kurt trocken zum Schluss, wobei er allerdings nicht einen römischen Kaiser, sondern seinen Mathematiklehrer aus seiner Schulzeit zitierte.

Nigel Coombs, Pensionist (ehemals KPMG Lausanne)

Résumé d'un mélodrame informatique en cinq actes

Où l'on découvre que le véritable danger ne vient ni de l'extérieur, ni des hackers, ni de la base de données *Oracle*, ni du système d'exploitation VAX, ni d'un virus mais de l'intérieur comme le montrent toutes les statistiques.

L'épilogue de ce mélodrame montre que toute politique de sécurité informatique repose sur une formation et une sensibilisation des utilisateurs complétées par le recours à des moyens techniques appropriés. Le point faible demeure la gestion des mots de passe et le manque d'attention portée aux messages d'erreurs du système.

Computerkriminalität

Computerviren so schlimm wie Erdbeben!

Die Swiss Re schätzt, dass der Computervirus "I love you" im letzten Jahr einen Schaden von rund 2.6 Milliarden US Dollar verursachte. Die Swiss Re kategorisiert die Schadenfälle u.a. in Katastrophenfälle. Im Jahr 2000 beliefen sich diese auf rund 50 Milliarden US Dollar. Nach acht Naturkatastrophen rangiert "I love you" auf Rang neun in dieser Kategorie!

Es handelt sich dabei um Statistiken von Swiss Re, nicht um Versicherungsmeldungen. (Anmerkung der Red.: Diese selbst treffen nämlich beim Rückversicherer häufig erst mit Verspätung ein…)

Quelle: www.swissre.com/e/publications/

Es ist nicht bekannt, dass es bis heute ein Krimineller geschafft hätte, Schäden zu verursachen, die mit Naturkatastrophen zu vergleichen sind. Offenbar sind wir jetzt so weit. Ein Grund mehr für den IT-Auditor, sein Augenmerk auf die Sicherheit im Umfeld der IT zu konzentrieren.

A Final Word of Password Wisdom

Passwords are like underwear: Don't share them, and above all, change them frequently.

(Copied from a Mexican Hackers Emergency Response Team Bulletin Board)