Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Band: 83 (2005)

Heft: 3

Artikel: ICT : was zu erhöhtem Risiko führt

Autor: Bernhart, Christian

DOI: https://doi.org/10.5169/seals-877111

ICT – was zu erhöhtem Risiko führt

CHRISTIAN BERNHART **Der Mensch und nicht etwa die Technik bleibt der grösste Risikofaktor in der Sicherheit und Verfügbarkeit der Informations- und Kommunikationstechnologie. Nicht die Hacker von aussen, sondern die naiven Benützer in den Betrieben selbst bergen das grösste Gefahrenpotenzial, vertritt Thomas Schlienger, Assistent am International Institute of Management in Telecommunications (iimt) der Universität Freiburg.**

Die geeigneten Tools für das umfassende Sicherheitsmanagement in der Informations- und Kommunikationstechnologie (ICT) sind durchaus vorhanden, doch werden sie zum Teil nicht eingesetzt, einerseits aus Bequemlichkeit und andererseits der knappen Finanzen wegen. Dies ist eine der Schlussfolgerungen, zu der Thomas Schlienger in seiner, kurz vor Abschluss stehenden Doktorarbeit kommt.

Das Kernproblem

Nicht die Technik an sich ist das Kernproblem, sondern deren Vernachlässigung. Diese fängt schon im Kleinen an. «Wir stellen immer noch fest, dass viele privaten Benützer, aber auch Firmen, Organisationen und Vereine die einfachsten technischen Hilfsmittel wie Firewalls oder Virenscanner schlecht oder gar nicht einsetzen», erläutert Thomas Schlienger. Mangelnder Einsatz der Tools heisst auch, dass Betriebssysteme und Virenscanner nicht aktualisiert werden. Es genügt vielfach auch nicht, ein verhältnismässig günstiges Viren-Update anzuschaffen. Es kann sich nämlich herausstellen, dass der in die Jahre gekommene Rechner einen begrenzten Arbeitsspeicher hat oder das betagte Betriebssystem das Update nicht mehr unterstützen kann.

Kosten sparen am falschen Ort

Der Grund hinter der mangelnden Sicherheitstechnik in den Betrieben ist oft auf das reduzierte Informatikbudget zurückzuführen. Thomas Schlienger weist dabei auf eine Gegenreaktion hin. Im Zug der Euphorie des E-Business habe man die ICT-Budgets zuerst aufgestockt. Nach dem ernüchternden Verlauf mit Korrekturen beim E-Banking (von Tobel), Yellowworld (Post) und auch beim Bund seien diese Budgets wieder zurückgestuft worden. Unter dieser Korrektur leide auch das Sicherheitsbudget massiv, vor allem deshalb, weil mit Informatiksicherheit kein Gewinn zu erzielen ist. «Damit lässt sich nur ein potenzielles Risiko reduzieren. Das bewirkt, dass eine solche Investition nur schwer an den Mann gebracht werden kann», erläutert Thomas Schlienger. Demzufolge werden die Sicherheitsmassnahmen nicht mehr auf den letzten Stand gebracht, und der Schutz gilt nur noch für die Risiken von gestern. Aber das gekappte Budget führt nicht nur zur Reduktion der Sicherheitstechnik. Thomas Schlienger hat beobachtet, dass die Budgetreduktion ebenso die Ausbildung betrifft und dass noch eine Reduktion der Informatik-Mitarbeitenden hinzukommt. Wenn weniger Mitarbeiter mehr Plattformen als vorher betreuen müssen, sind als Folge davon mehr Lücken im Sicherheitssystem zu verzeichnen.

Neue Technologien, neue Risiken

Es kommt hinzu, dass die Einführung neuer Anwendungen und Techniken immer auch neue Risiken mit sich bringt. Der bereits weit verbreitete Zugang in das Internet per Funk beispielsweise hat zur Folge, dass die meisten Benützer sich mit ihren Notebooks und Labtops unnötig entblössen. Ihr Wireless-LAN-Anschluss ist nämlich durch den Standardschutz des Wired Equivalency Privacy (WEP) nur vermeintlich geschützt, weil dessen Code schon vor Jahren geknackt worden ist. Das Surfen durch fremde Internetzugänge ist dank dem Dienst von www.wardriving.ch besonders unter Studenten zum adretten Zeitvertreib geworden.

Die technische Entwicklung mit der enorm gestiegenen Zahl an Daten hat auch beim Backup zu Risikoproblemen geführt. Der Datenstrom ist derart angestiegen, dass er vielerorts nicht mehr aktuell gesichert wird. Verhängnisvoll wurde dies beispielsweise am 23. Juli 2003 für viele KMU-Kunden, die ihren E-Mail-Verkehr an das Weboffice von Sunrise ausgelagert hatten. Dabei war das Storage-System von Sunrise zusammengebrochen, E-Mails gingen unwiederbringlich verloren.

Eine Verfügbarkeit der Daten zu 99,9% ist äusserst kostspielig und ist in vielen Informatiklösungen deshalb auch nicht inbegriffen. Thomas Schlienger weist in diesem Zusammenhang auf die bei Grossbanken von zu Zeit zu Zeit aufbrechende Diskussion hin, die in der Kernfrage mündet, ob es realistisch sei, dass eine Bank Konkurs anmelden müsse, wenn die ICT-Infrastruktur für einen Tag ausfalle. Die Frage ist nicht zu beantworten, weil bis jetzt noch kein solcher Fall eingetroffen ist. Die Wahrscheinlichkeit, dass ein solcher Fall – ausgelöst etwa durch ein gigantisches Bombenattentat, einen ausserordentlichen Sabotageakt oder ein Erdbeben – eintrifft, ist so klein, dass die enormen Investitionen, um dieses Risiko zu senken, gar nicht in Erwägung gezogen werden.

Sicherheitsfaktor Mensch

Die Sicherheit und Verfügbarkeit der ICT in den Betrieben hängt aber gemäss den Untersuchungen von Thomas Schlienger nicht in erster Linie von den fehlenden techni-

Der Mensch und nicht die Technik ist der grösste Risikofaktor in der Sicherheit der ICT.

schen Installationen ab, sondern lässt sich oft auf das mangelnde Verhalten der Mitarbeitenden zurückführen. So ist die Verletzbarkeit von aussen über das Internet durch Hacker nur in seltenen Fällen systembedingt. Beispielsweise sind Online-Dienste verletzlich, wenn ihr Dienst von Erpressern systematisch sabotiert wird. Dies geschah an den Fussball-Europameisterschaften, als Wettbüros erpresst wurden mit der Drohung, den Online-Tipp-Service mit Massenanfragen zu blockieren, falls nicht ein gewisser Betrag bezahlt würde. Webdienste sind verletzlich, weil Webserver so blockiert werden können, dass sich ein gewöhnlicher Datenverkehr darüber nicht mehr abwickeln lässt.

«Das Risiko von Hackern, die über das Internet in das System gelangen, wird immer etwas zu gross eingestuft», meint Thomas Schlienger. «Die grösste Gefahr kommt vom Betrieb, von der Firma oder Organisation selbst und nicht von aussen. Das Problem der Viren besteht darin, dass sie sich innerhalb von ein bis zwei Stunden über die ganze Welt verbreiten können. Ein Virenscanner, der nicht aktuell ist, wird kaum Schutz bieten. Im Virenschutz muss die Reaktionszeit in der Tat verbessert werden.» Das grössere Problem sei das oft geradezu von erstaunlicher Naivität zeugende Verhalten der Informatikbenutzer. Während heute die meisten Leute gegenüber unbekannten Briefen skeptisch reagieren, neigen viele unter ihnen noch dazu die E-Mails oder Attachements von unbekannten Absendern sorglos zu öffnen. Auf diese Weise konnte sich beispielsweise der «I love you»-Virus in Windeseile fortpflanzen. Zurzeit, so Thomas Schlienger, sei vor allem in Deutschland eine Übertölpelungsaktion naiver Internet-Bankkunden im Gange. Dabei werden sie in einer E-Mail im Namen der Bank aufgefordert, das Login, Passwort und den Transaktions-Code anzugeben, damit die Bank die Authentizität der Person überprüfen kann. Auf diese Weise wollen Betrüger an die Codes naiver Kunden herankommen und dann das Geld auf deren Bank abheben. Diese Attacken werden Pishing genannt, ein Wortkonstrukt aus «Password fishing».

Das Problem des naiven Benutzers, der seinen elektronischen Schlüssel sorglos abgibt, wäre im Grunde genommen über einen Personal-Key-Identifikator (PKI) zu lösen. Das Gesetz dazu existiert in der Schweiz, noch aber fehlt es an einer Zertifikationsstelle. Die Erfahrung in anderen Staaten – beispielsweise in Finnland, wo der Staat diesen Dienst anbietet – zeigt jedoch, dass erst wenige Personen davon Gebrauch machen. Die beste Sicherheit, vertritt Thomas Schlienger, gibt es nicht, der PKI wäre jedoch eine gute Sicherheit im Verkehr heikler Daten. Doch bereits die heute bestehenden elektronischen Bankverbindungen seien so gut verschlüsselt und dank den Transaktionsnummern praktisch unmöglich zu knacken. Jede technische Massnahme nütze aber nichts, wenn der Benutzer die Sicherheitseinrichtungen preisgibt.

Sicherheitsmassnahmen

Welche Massnahmen müsste heute ein Betrieb einleiten, damit bei der ICT die Sicherheit und Verfügbarkeit auf einem guten Standard sind? Aufgrund seiner Erfahrung und Recherchen für seine Doktorarbeit spricht Thomas Schlienger von drei Bereichen:

- Einführung von Grundschutzmassnahmen, wie es ISO-17799 vorsieht
- Prozessanalyse der Informatik im Hinblick auf Sicherheitsmängel
- Sensibilisierung und permanenten Ausbildung der Mitarbeiter

Sicherheitsstandards

Eine gute Grundlage für die Einführung von ICT-Sicherheitsstandards als «Best Practice Approach» stellen beispielsweise jene Massnahmen dar, die das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) im Grundschutzhandbuch vorschlägt. Gut fährt ebenfalls, wer die Grundschutzmassnahmen aus den zehn Bereichen befolgt, die der ISO-17799 als Standards aufstellt. Werden diese Standards flächendeckend installiert, so verfügt man über eine gewisse Grundsicherheit. Eine eigentliches Zertifizierungsverfahren ist dabei nicht Voraussetzung. Der Standard kann online über die Schweizer Normenvereinigung zu

einem Preis von 200 Franken in Englisch erworben werden. Werden die zehn Bereiche, wie Datenzugriff, Ausbildung oder Sicherheitspolitik, als Checkliste durchgegangen und – so es für den Betrieb sinnvoll ist – implementiert, dann können damit die gravierendsten Lücken behoben werden. Laut Thomas Schlienger muss man dank diesem Vorgehen vor allem keine eigenen Sicherheitsstandards entwickeln.

Prozessanalyse

Die zweite Massnahme liegt im organisatorischen Bereich. Erst eine Prozessbeschreibung mit der Analyse des Datenflusses ermöglicht ein Sicherheitsgesamtkonzept. Mit der Prozessbeschreibung werden zuerst jene Stellen mit den sensiblen Daten erfasst. Die Analyse ermöglicht es, Fehler und Sicherheitsmängel an spezifischen Orten aufzudecken. «Vielleicht stellt es sich dann heraus», erklärt Thomas Schlienger, «dass nur gewisse Bereiche mit besonderen Massnahmen zu schützen sind.» Sicherheit werde leider oft sehr unsystematisch angegangen, indem man hier und dort einen Firewall oder einen Virenscanner installiert. «Hier muss man aber in die Details gehen, es nützt nichts, einen Wildwuchs von Sicherheitstechnik ohne Gesamtkonzept zu haben», vertritt Thomas Schlienger. Mit unsystematischen Installationen kann nämlich auch der interne Datenfluss gestört oder blockiert werden.

Mitarbeiterschulung

Der dritte Bereich betreffen die Mitarbeiter, die für Sicherheitsanliegen zuerst sensibilisiert und für gewisse Tools geschult werden müssen. Tatsache ist, laut Thomas Schlienger, dass in vielen Betrieben die meisten Mitarbeiter nur über ein sehr selektives Informatik-Know-how verfügen. Dies macht sich oft dann negativ bemerkbar, wenn E-Mails arglos geöffnet werden oder Sicherheits-, bzw. Verschlüsselungsprodukte gar nicht erst installiert werden. Zwei Mängel stellt Thomas Schlienger in diesem Bereich fest. Die betreffenden Produkte sind oft benutzerunfreundlich, das heisst, man muss viel Zeit investieren, um sie nutzen zu können. Andererseits bemühen sich die Benutzer deswegen auch zu wenig, diese Produkte nutzbar zu machen. Hier schleicht sich gerade im E-Mail-Verkehr ein technisches Problem ein. Zum Schutz der sorglosen Benützer richten die Systemadministratoren oft einen rigorosen Spam- und Virenschutz ein, mit der Folge, dass viele legitime E-Mails den Adressaten nicht mehr erreichen und an den Absender zurückgeschickt werden.

Der Wirtschaftsinformatiker Thomas Schlienger (35) arbeitet als Forschungsassistent am International Institute of Management in Telecommunications (iimt) der Universität Freiburg, wo er zurzeit seine Doktorarbeit über die Sicherheit und Verfügbarkeit in der Informations- und Kommunikationstechnologie schreibt. Sein Diplom für Informationsmanagement erwarb sich Thomas Schlienger an der Universität Zürich und war danach während ein paar Jahren Projektmanager bei Compudata im Bereich Data Interchange (EDI) and E-Government Projects tätig.

Info: Thomas Schlienger, Tel. 026 300 84 28, thomas-schlienger@unifr.ch, www.iimt.ch

Generell hat Thomas Schlienger durch die Forschung für seine Doktorarbeit festgestellt, dass die Sensibilisierung und Ausbildung für die Sicherheit recht spät greifen. Während Sicherheit in anderen Verkehrsströmen, beispielsweise auf der Strasse oder auch im sexuellen Bereich, schon früh während der Schulzeit – für den Strassenverkehr bereits im Kindergarten – als wichtiges Thema zur Sprache kommt, wird Informatiksicherheit erst in den Betrieben, wenn überhaupt, thematisiert und eingeführt. «Dieser Informations- und Vermittlungsprozess fängt sehr spät an und sollte bereits in den Schulen beginnen», verficht Thomas Schlienger. Er plädiert zudem, dass beim ersten Umgang mit dem Computer Sicherheitsrisiken ein Thema sein sollte. Ein Standardlernkompendium in Sicherheit sollte dazu gehören, keines mit allen Details, aber eines mit einer grundsätzlichen Sensibilisierung für gewisse Risiken.

Sicherheit im Wandel der Zeit

In den letzten 30 Jahren, vor allem seit der grossflächigen Einführung der Computertechnik haben sich die Sicherheitskonzepte markant geändert. In den 70er- und anfangs der 80er-Jahre wurde die Sicherheit vor allem in technischer Hinsicht angegangen, weil sich damals die meisten Computer in Rechnungszentren befanden und von Technikern für Techniker betrieben wurden. Dies hat sich seit Mitte der 80er-Jahre, als der PC auf das Pult der Sekretärin kam, radikal geändert. Man realisierte, dass dafür Richtlinien zur Handhabung der Computer zu erstellen und einzurichten waren und dass es für die Sicherheit auch verantwortliche Personen braucht.

Jede neue ICT-Anwendung, so Thomas Schlienger, ruft wieder nach neuen Sicherheitskonzepten und Lösungen. Die Tendenz zur Auslagerung hat beispielsweise ein neues Sicherheitsdenken bei der physischen Vernetzung nach sich gezogen. Bei den Leitungen könnte ein Engpass entstehen, deshalb sollten sie redundant angelegt werden, was aus Kostengründen nicht immer der Fall ist. Oder im Gesundheitswesen wird gegenwärtig diskutiert, wie die Patientendaten auf welche Datenbanken zu verteilen sind, damit einem Missbrauch Vorschub geleistet werden kann. Dass die Datenhoheit beim Patienten liegen soll, wird allgemein befürwortet. Das dabei vorgeschlagene Prinzip des doppelten Schlüssels, mit lückenlosen Benutzermeldungen nach dem «vitrine brisée»-Prinzip findet Thomas Schlienger als vertretbare Lösung, weil dann der Patient bei Missbrauch klagen kann. Die Absicht sei gut, die Praxis aber werde erst zeigen, ob dieses Prinzip gewisse Patienten nicht überfordern wird.

Jede ICT-Weiterentwicklung wird unumstösslich neue Aspekte der Sicherheitsproblematik aufzeigen. Ein grundliegendes Problem liegt für Thomas Schlienger jedoch darin, dass Sicherheitsmassnahmen meist reaktiv und nicht proaktiv vorgenommen werden. «Deshalb», sinniert der in diesen Fragen bestens bewanderte Informatiker, «haben es Sicherheitschefs gern, wenn ab und zu etwas passiert. Erst dann können sie mit Erfolg auf grössere Sicherheitsvorkehrungen pochen.»

Zusammengefasst kann festgehalten werden, dass fehlende Prozessanalysen, naive Benutzer und gekappte Budgets das Risiko erhöhen. ■