Zur IT-Sicherheit am RRZN und an der Uni Hannover

Mit Inbetriebnahme der ersten Rechnerausstattung des RRZN im Jahre 1973 (Control Data CYBER 76 und 2 * CYBER 73) begannen gegenüber der bis dahin betriebenen Rechenanlage (Control Data 1604-A und 8090) auch in Hannover moderne Zeiten: Mehrere Programme konnten nun simultan auf den Rechnern bearbeitet werden, und die Datenhaltung erfolgte für alle Benutzer online auf (seinerzeit) großen Magnetplatten.
Es zeigte sich nach einiger Zeit, dass damit eine neue Klasse von Problemen auftrat: Durch Fehler in Programmen und/oder im System oder auch durch Mängel im Design der Betriebssoftware sowie auch durch unbedachtes Verhalten der Benutzer konnten Dritte in den Besitz von Informationen gelangen (beispielsweise fremde Passwörter), die sie nicht haben sollten. Im Laufe der Jahre nahm auch die Bedeutung der Viren-Problematik auf den PCs zu. Diese Entwicklungen waren – etwas verallgemeinert gesagt – die Geburtszeit der Begriffe der IT-Sicherheit und des Datenschutzes. So war das RRZN relativ früh mit IT-Sicherheit befasst und bearbeitete sie im Rahmen der System-Unterstützung standardmäßig durch Verfolgung/Untersuchung von „Sicherheitslöchern" der Systemhersteller bzw. sowie Installation und Bereitstellung/Verteilung von sicherheitsbezogenen Updates der Software--Hersteller.

Jedoch zeigte sich mit der Zeit, dass Angriffe immer komplexer und deren Abwehr bzw. Schadenbeseitigung immer aufwendiger wurden, sodass die erforderlichen Arbeiten im Rahmen der traditionellen Systempflege nicht mehr hinreichend zu leisten waren. Auch das zunehmend breitere Spektrum der div. Sicherheitsaspekte erforderte Maßnahmen, die den Rahmen der Systempflege signifikant überschritten. Zugleich wurde mit der Zeit auch immer deutlicher, dass Angelegenheiten der Sicherheit nicht mehr nur für einzelne Benutzer bzw. Rechner des RRZN und/oder der Institute (inkl. der jeweiligen Netze), sondern auch universitätsweit (und ggfs. sogar darüber hinaus) relevant wurden. Daher lag es nahe, das Thema „IT-Sicherheit" für die Universität Hannover grundsätzlich anzugehen.

Aus dieser Erkenntnis heraus wurde 1997 im Rahmen einer größeren Umorganisation im RRZN eine **Stabsstelle „IT-Sicherheit"** eingerichtet. Damit war es möglich, die Thematik „IT-Sicherheit" auf eine wesentlich breitere Basis als bisher zu stellen (positiv wirkte sich auch aus, dass in Zusammenhang mit Sicherheitsarbeiten für die Uni-Verwaltung das für die Sicherheit tätige Personal aufgestockt werden konnte). Um die Verfolgung dieses Ziels möglichst bald in hinreichender Breite umsetzen zu können, erfolgte eine Anlehnung an das Bundesamt für Sicherheit in der Informationstechnik (BSI): Durch Befassung mit dem Grundschutzhandbuch und durch Teilnahme an etlichen BSI-Veranstaltungen (Kongresse, Seminare, Lehrgänge) stand das dort vorhandene Know-how relativ kurzfristig gewinnbringend für die Universität zur Verfügung.

Eine der ersten wesentlichen Erkenntnisse: IT-Sicherheit ist nicht nur eine technische und mentale Aufgabenstellung, sondern im Wesentlichen auch eine organisatorische: für ein umfassendes Konzept und den Einsatz wirkungsvoller Maßnahmen sind **spezifische Verantwortungsstrukturen** notwendig! Dies gilt insbesondere auch im Hinblick auf den vom BSI inhaltlich geprägten Begriff der IT-Sicherheit, der sich in Erweiterung der bisherigen Sichtweise (wie Programmfehler, Designmängel) an der verlässlichen Verfügbarkeit von Diensten aus Anwendersicht orientiert.

Hand in Hand mit dieser Erkenntnis ging einher die Notwendigkeit zur **Förderung des Sicherheitsbewusstseins** in den Instituten der UH sowie in der Benutzerschaft des RRZN allgemein. Zu diesem Zweck wurden etliche Institute, die von Sicherheitsvorfällen betroffen waren, besucht und vor Ort Empfehlungen zum weiteren Vorgehen erörtert.

Sicherheit für Verwaltung der UH

Aktivitäten der Verwaltung der UH mit dem Ziel, spezifische Abläufe der UH zu digitalisieren, führten naturgemäß zu einer Reihe von sicherheitsbezogenen Aspekten, in die das RRZN involviert war.
Hieraus ergaben sich im Prinzip zwei Anforderungen:

1) Weltweite Zugriffsmöglichkeiten auf Systeme/Services im Verwaltungsnetz (beispielsweise für Rückmeldungen der Studierenden)
2) Direkter Zugriff z.B. auf Software der UH-Verwaltung seitens entsprechend privilegiertem Institutspersonal (z.B. für Buchungen)

Für diese Art der Aufgaben waren entsprechende und angemessene Lösungen zur IT-Sicherheit zu finden. Zu 1) wurde ein leistungsfähiges Firewall-System, zu 2) wurde eine Chipkarten-basierte Sicherheitslösung konzipiert, installiert und in Betrieb genommen.
Die resultierenden Arbeiten waren - vorab erkennbar - relativ personalintensiv, sodass dem RRZN zusätzliche Personalstellen für Belange der UH-Verwaltung/IT-Sicherheit bewilligt wurden.

Sicherheitstage

Aus der Erkenntnis heraus, dass etliche Sicherheitsaspekte in den Systemen je nach individueller Konfiguration von Hard- und Software aufeinander aufbauen oder auch ineinandergreifen, schien es sinnvoll zu sein, in mehrtägigen Veranstaltungen eine Reihe unterschiedlicher, aber verwandter Sicherheitsthemen zu behandeln. Dazu konnten auch Dozenten von anderen Hochschulen und vom DFN-CERT Hamburg gewonnen werden. So wurden im Jahr 2001 die „**Sicherheitstage“** für Benutzer, insbesondere Administratoren, ins Leben gerufen. Eingespielt hat sich im Laufe der Jahre, dass die Sicherheitstage einmal jährlich im Wintersemester mit wechselndem Programm jeweils im Umfang von ca. drei Tagen Dauer angeboten und auch gut angenommen wurden.

Arbeitsgruppe „IT-Sicherheit“ der Senatskommission

Um die Thematik IT-Sicherheit in der Universität wirkungsvoller vertreten und verbreiten zu können, wurde in der für das RRZN zuständigen Senatskommission eine **Arbeitsgruppe „IT-Sicherheit“** eingesetzt mit Federführung beim RRZN. Anlässlich grundsätzlicher Diskussionen über Sicherheitsmaßnahmen und die Möglichkeiten zu deren Um-/Durchsetzung in der UH wurde die Notwendigkeit erkannt, eine **Ordnung zur IT-Sicherheit** vom Senat verabschieden zu lassen und damit universitätsweit bindend zu machen. Die Arbeitsgruppe setzte sich daher das Ziel, eine derartige Ordnung zu erstellen. Da trotz etlicher Recherchen ein irgendwie geartetes „Vorbild“ für eine solche Ordnung nicht gefunden werden konnte, wurde sie sozusagen „von null an“ entwickelt. Eine derartige Ordnung, die u.a. eine IT-Sicherheits-Verantwortungsstruktur in die Universität einzieht (Zentraler Sicherheits-

beauftragter, von den Instituten zu benennende dezentrale Sicherheitsbeauftragte, Rolle des RRZN) konnte im Juli 2002 vom Senat verabschiedet werden. Deren praktische Umsetzung wurde mit dem Einsetzen des Zentralen Sicherheitsbeauftragten im Dezember 2003 aufgenommen.

Zertifizierungsstelle

Einem sich abzeichnenden Bedarf an erhöhter Sicherheit durch Einsatz von PKI-Strukturen (Public Key Infrastructures) entsprechend wurden Untersuchungen zum Aufbau einer CA (Certification Authority) eingeleitet; auch wurde eine Diplomarbeit zu dieser Thematik betreut. Eine intensivere Befassung mit dieser Materie war ab 2001 möglich. Als wesentliche Grundlage fungierte dabei das Deutsche Signaturgesetz, das Struktur und Orientierung in die Materie brachte. Es fand ein intensiver Gedankenaustausch mit dem DFN-CERT in Hamburg statt, das auf dem gleichen Gebiet arbeitete. Dabei war uns ziemlich bald bewusst, dass das RRZN die Anforderungen des Signaturgesetzes für einen CA-Betrieb nicht erfüllen und deswegen nur „minderwertige“ Zertifikate ausstellen konnte. Mit Aufnahme eines ersten Probebetriebs zur Ausstellung von Zertifikaten zeigte sich ein reges Interesse in der Benutzerschaft. Im Sinne des weiteren Fortschritts war es dann sehr hilfreich, dass das DFN-CERT seine Arbeiten zur Bereitstellung von Zertifizierungsdiensten für die Deutschen Hochschulen so weit vorangetrieben hatte, dass ebenfalls erster Betrieb möglich war. So gelangte eine vom DFN-CERT strukturell vorgesehene Aufteilung zum Einsatz: Das DFN-CERT fungiert als CA, das RRZN übernimmt die Rolle einer RA (Registration Authority) an dieser CA. RRZN-Benutzer beantragen Zertifikate bei der RA am RRZN, und die DFN-CERT CA stellt die nach Signaturgesetz qualifizierten Zertifikate aus.
Mit dieser Konstellation wurde dann der Benutzerbetrieb mit „neuen“ Zertifikaten aufgenommen, während der ursprüngliche Service mit RRZN-seitigen Zertifikaten nach und nach abgebaut wurde.

Absolut einmalig: Das Jahr-2000-Problem

Wer erinnert sich noch daran? Die aus der Anfangszeit der Computer stammende Programmier-Gepflogenheit, Datumsangaben mit nur 2-stelligen Jahreszahlen vorzunehmen, drohte ab 1.1.2000 zu einer bösen Falle zu werden: Die Jahreszahlen waren nicht mehr eindeutig, Datumsdifferenzen möglicherweise um 100 Jahre falsch! Die Konsequenzen können vergleichsweise dramatisch sein…! Da Datumsoperationen auf allen Ebenen (auch systemintern von Treibern bis hinauf zur Anwendungsebene) stattfinden können, gibt es kein automatisches Verfahren, um alle möglichen Schwachstellen beseitigen zu können. Vielmehr musste in jedem Einzelfall eine individuelle Analyse und dann eine angemessene Korrektur vorgenommen werden. Das hat im Vorfeld des „Jahrtausend-Wechsels“ teilweise zu erheblichem Umstellungsaufwand bei Herstellern, aber auch vor Ort an Rechenzentren geführt, zumal der 31.12.1999 die **absolute** Deadline war (keinerlei Aufschub möglich!).

Auch am RRZN musste man sich mit dieser Thematik befassen. Da sich, wie bereits weiter oben erwähnt, der Begriff der IT-Sicherheit auch auf die **Verfügbarkeit** der angebotenen Dienste bezieht, führte diese Definition dazu, dass die Zuständigkeit für das Jahr2000-

Problem am RRZN der Gruppe IT-Sicherheit zufiel. Die Erkenntnisse zu dieser Thematik schlugen sich u.a. in einem in der BI veröffentlichten Grundsatzartikel mit einer Reihe von Erläuterungen und Empfehlungen für Benutzer nieder (Dieser Artikel wurde auch von einer größeren Anzahl von Rechenzentren anderer Hochschulen nachgedruckt). Die konkreten Vorbereitungen zum Jahrtausend-Wechsel waren insofern erfolgreich, als dem RRZN im Zusammenhang mit dem konkreten Übergang vom 31.12.1999 auf den 1.1.2000 keine Probleme bekannt geworden sind.
Wie schon gesagt: Das Jahr-2000-Problem war einmalig … fast. Die nächste Komplikation dieser Art (abgesehen von möglichen Unix-Problemen in den Jahren 2036 bis 2038) ist im Jahr 9999 zu erwarten – noch eine Weile hin…

Ausstrahlung des RRZN auf andere Institutionen

Die am RRZN durchgeführten Arbeiten bzw. deren Ergebnisse erlangten mit der Zeit auch **regional** und **überregional** an Bedeutung.

Im damaligen **Niedersächsischen Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren** (NALWR) befasste sich eine Arbeitsgruppe, der Vertreter der Hochschulen Niedersachsens angehörten, mit der Netzthematik und behandelte ursprünglich in diesem Zusammenhang auch Sicherheitsfragen. Anlässlich der zunehmenden Bedeutung und des ständig wachsenden Umfangs der Sicherheitsthematik wurde diese in eine eigene Arbeitsgruppe ausgegliedert (Federführung beim RRZN). In den Diskussionen (z.B. über die Sicherheitsordnung, Einrichtung einer CA, besondere Sicherheitsvorfälle) zeigte sich immer wieder, dass Erkenntnisse bzw. Anregungen des RRZN durchweg begrüßt wurden, da an den anderen Hochschulen nur eine vergleichsweise beschränkte personelle Kapazität für IT-Sicherheit einsetzbar war.

IT-Sicherheit in der Landesverwaltung

Im Nds. Innenministerium wurde im Jahr 2004 eine Arbeitsgruppe zur Erstellung eines Sicherheitskonzepts für die Nds. Landesverwaltung ins Leben gerufen. In diesem Zusammenhang wurde das RRZN gebeten, eine Präsentation bezüglich der Sicherheitsordnung der UH zu geben. Obwohl diese Ordnung naturgemäß nicht direkt auf die Belange der Ministerien abbildbar war, konnten jedoch wesentliche Prinzipien verdeutlicht werden, die beim Aufstellen einer Ordnung bzw. eines Sicherheitskonzepts zu berücksichtigen sind (z.B. Verantwortungsstrukturen, „Sicherheit ist Chefsache“). Resultat: Das RRZN wurde gebeten, in der Arbeitsgruppe beratend mitzuwirken bzw. an deren Sitzungen teilzunehmen. Dies geschah durch den Chronisten bis zu seiner Pensionierung.

Arbeitskreis „Informationssicherheit“ des ZKI.

Das RRZN war naturgemäß auch Mitglied im ZKI (ZKI: „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.“, siehe auch www.zki.de.). Mit einem Vortrag beim ZKI im Herbst 2004 wurde die „Ordnung zur IT-Sicherheit an der Universität Hannover“ vorgestellt. Der Arbeitskreis „Informationssicherheit“ des ZKI, der zur damaligen

Zeit umfassende Empfehlungen zur IT-Sicherheit an deutschen Hochschulen erarbeitete, nahm daraufhin die hannoversche Ordnung als Vorlage für seine „Musterordnung“. (Auf der entsprechenden Webseite des ZKI aus dem Jahr 2005 war als Fußnote 6 vermerkt: „Als Vorlage für die zwei Muster diente die Ordnung aus Hannover… .“ Diese Webseite ging im September 2020 auf in den Weiterentwicklungen „IT-Grundschutz-Profil für Hochschulen“ und „Baustein-Kommentierungen zum IT-Grundschutz-Profil“, die in Zusammenarbeit zwischen ZKI und dem BSI erarbeitet wurden).

Schlussbemerkung

Dieser Übersichtsbericht endet mit der Pensionierung des Chronisten Ende Oktober 2005. Wie sich die Dinge weiterentwickelt haben, mögen Interessierte aktuellen einschlägigen Webseiten entnehmen.

Mit den eingeführten Maßnahmen ist das Ziel näher gerückt, ein Sicherheitsniveau entsprechend dem vom BSI definierten Grundschutz zu realisieren. Mit der Erkenntnis „IT-Sicherheit ist kein Zustand, sondern ein Prozess“ und sich daraus ergebender Empfehlung zu Weiterentwicklungen wird es möglich sein, das RRZN (das seit einiger Zeit nach Willen der Universität Hannover leider nicht mehr so heißen darf) und die Universität Hannover bezüglich der Anforderungen der IT-Sicherheit in guter Position zu halten.

Hans-Jürgen Hille