Privacy Respecting Incident Management

Beitrag zur Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V.

Ursula Sury

Organisatorische und juristische Implikationen bei der datenschutzgerechten Nutzung bzw. Durchführung des Einsatzes von Intrusion Detection

ABSTRACT

Um den Anforderungen der Informatiksicherheit gerecht zu werden, werden durch IT-Systemverantwortliche immer häufiger Intrusion Detection Systeme (IDS) eingesetzt. Dies ist im Sinne einer sorgfältigen und verantwortlichen Unternehmensführung sinnvoll und gefordert, der konkrete Einsatz wirft aber verschiedene Fragen des Datenschutzes auf.

Mit einem technisch korrekten und datenschutzrechtlich begründeten Einsatz von IDS lässt sich der Zielkonflikt zwischen dem Anspruch an Forensic einerseits und informationeller Selbstbestimmung andererseits auflösen.

1. Intrusion Detection Systeme

Unter **Intrusion** versteht man die nicht autorisierte Bedrohung der IT-Ressourcen durch einen Angreifer beispielsweise durch einen Hacker. Unter **Intrusion Detection** versteht man somit sämtliche Vorkehrungen, die böswillige Aktivitäten gegen die eigenen eingesetzten IT-Ressourcen feststellen, und sämtliche daraus folgenden Aktivitäten zur Vermeidung grösseren Schadens und Behebung von Lücken etc. (vgl. dazu Northcutt Stephen/Novak Judy, Intrusion Detection-Systeme, Spurensuche im Internet, Deutsche Ausgabe, Bonn 2001).

Der Intrusion Detection Prozess besteht einerseits in der eigentlichen **Detection**, d.h. dem Aufdecken von Angriffen gegebenenfalls verbunden mit der Sammlung der notwendigen Informationen und der Analyse des Angriffs. Zum anderen zählt zum ID-Prozess die Reaktion, d.h. die Antwort, sogenannte Intrusion **Response**, falls das System Alarm schlägt oder gegebenenfalls automatisch auf Angriffe reagiert und auch verantwortliche Personen rechtliche, technische und organisatorische Massnahmen treffen.

Intrusion Detection Systeme, kurz IDS genannt, sind spezielle Sicherheitsmanagementsoftwarewerkzeuge, welche im Intrusion Detection Prozess eingesetzt werden. Verschiedene IDS-Softwareprodukte sind schon seit längerem auf dem Markt erhältlich, deren Qualität und somit Aussagekraft wird aber häufig diskutiert.
IDS-Meldungen, welche fälschlicherweise als Angriffe durch das System taxiert werden, werden als **False Positives** bezeichnet. Als **False Negatives** werden tatsächliche Angriffe bezeichnet, die das IDS nicht erkennt.

IDS überwachen den Netzwerkverkehr mit dem Fokus, Unregelmässigkeiten festzustellen, um Hacken, die Einschleusung von Malware oder den Missbrauch bestehender Dienste (http-Tunnel), zu verhindern oder eben sofort darauf reagieren zu können. Der Fokus ist also, anders als beim Einsatz von Spam, nicht auf die Überprüfung von Inhalten (Wörter, Bilder) gerichtet.

2. Einordnung der Intrusion Detection in die IT-Security

Sämtliche Vorkehrungen im Bereich Informatiksicherheit lassen sich chronologisch einteilen in den ersten Aspekt der Prävention, in den zweiten Aspekt der Detection und den dritten Aspekt der Repression (vgl. dazu Fuhrberg Kai/Häger Dirk/Wolf Stefan, Internet–Sicherheit, 3. Auflage, München 2001).

Unter **Prävention** versteht man sämtliche Vorkehrungen technischer, organisatorischer und rechtlicher Art, die getroffen werden müssen, um ein Maximum an Informatiksicherheit zu erreichen.

Zu den Handlungsfeldern der **Detection** zählen Vorkehrungen, um unberechtigte Angriffe auf IT-Ressourcen, die trotz einer sorgfältig umgesetzten Prävention geschehen und zum Teil auch Erfolg haben, rechtzeitig und möglichst beweisbar festzustellen und einem bestimmten Angreifer zuzuordnen.

Unter **Repression** versteht man sämtliche Aspekte der Informatiksicherheit, die dazu verwendet werden, erfolgte Angriffe zu ahnden, sei es auf dem Weg ziviler Haftpflichtansprüche, sei es, alternativ oder kumulativ, auf dem Weg der Durchsetzung staatlicher Strafansprüche.

Die Anwendung von Intrusion Detection ist grundsätzlich dem Handlungsfeld der Detection zuzuordnen; die Aspekte der Detection Response sind aber der Repression zuzuordnen.

3. Riskmanagement

3.1 Riskmanagement und IDS

Wer Riskmanagement betreibt, analysiert im obgenannten Sinn die möglichen Gefahren und bewertet diese nach **Schadengrösse**, **Schadensart** und **Eintrittswahrscheinlichkeit**. Als nächstes wird überlegt, welche Risiken sinnvollerweise zu **vermeiden** bzw. welche zu **vermindern** sind und welche man gegebenenfalls auf eine Drittperson **überwälzen** kann.

Zum Riskmanagement zählt auch die Planung, wie mit einer eingetretenen Krise korrekt umgegangen werden soll, damit der Schaden möglichst klein gehalten und aus dem eingetretenen Schaden für die Unternehmung viel gelernt werden kann. Es braucht folglich eine Überwachung sämtlicher möglicher Risikoherde und die Installation einer Krisenorganisation, die unverzüglich die Krise bewältigt. Die Überwachung impliziert dabei die Identifikation der Krise, aber auch deren Beurteilung resp. Bewertung, damit anschliessend die **adäquaten Bewältigungsmassnahmen** getroffen und umgesetzt werden können.

Der Einsatz von IDS dient im Bereich des Riskmanagementablaufs vor allem der Reaktion; wird über das Bestehen und den Einsatz eines IDS aber breit und rechtzeitig informiert, hat dies auch präventiven Charakter.

3.2 Versicherungen im IT-Umfeld

Eine mögliche Strategie, eingetretene Risiken zu überwälzen, ist der Abschluss von Versicherungen. Bei den Schäden in der Informationsgesellschaft handelt es sich in aller Regel um **Vermögensschäden**, die sehr gross sein können. Analysiert man die gängigen Standardprodukte der Versicherungsgesellschaften, so stellt man fest, dass reine Vermögensschäden kaum versicherbar sind, wenn diese aus dem Betrieb innerhalb der eigenen Unternehmung oder aus Nicht- und Schlechterfüllung von vertraglichen Verpflichtungen gegenüber Dritten entstehen. Wohl finden sich Angebote für den Abschluss von Versicherungen für Schäden an Hardware; will man diese aber auf die Übernahme von Schäden, die sich aus Datenverlusten ergeben, ausdehnen, stösst man auf Unverständnis. Selbst wenn sich die grundsätzliche Bereitschaft zur Übernahme gewisser, sehr eingeschränkter Vermögensschäden ergibt, sind die **Anforderungen betreffend Sorgfalt** an den Versicherungsnehmer so gross, dass die Wahrscheinlichkeit eines Schadeneintritts wieder gegen null tendiert.

Auch im Bereich des Underwriting bemühen sich die Versicherungen immer mehr, die Unternehmen zum Riskmanagement-Verhalten zu zwingen, werden diese doch sorgfältig geprüft, bevor man mit ihnen überhaupt gewisse Versicherungen abschliesst.

Auch unter dem Versicherungsaspekt, sei dies weil eben Versicherungen fehlen oder um Underwriting Anforderungen zu erfüllen, ist der sinnvolle Einsatz von IDS zu empfehlen.

4. Daten- und Persönlichkeitsschutz

4.1 Datenbearbeitung mit IDS

Intrusion Detection Systeme (IDS) **sammeln Daten** und bewahren diese sehr kurz auf (z.T. nur wenige Sekunden), bis der Analysevorgang abgeschlossen ist. Stellt das System einen Angriff fest oder glaubt es, einen solchen festgestellt zu haben, werden die Daten automatisch auf eine Disc kopiert, damit sie vom ID-Administrator analysiert und notwendige Massnahmen eingeleitet werden können. Selbstverständlich werden auch alle False Positives aufgezeichnet, dazu zählen vom System als ungewöhnlich taxierte Vorgänge, welche aber völlig unbedenklich sind wie zum Beispiel ein Up-Loading.

Viele dieser Daten lassen sich konkret den Internetbenutzern, also natürlichen Personen, zuordnen. Folglich werden mit IDS-Systemen Angaben, die sich auf bestimmte oder bestimmbare Personen beziehen, also **Personendaten**, bearbeitet.
Die gesammelten Informationen über Benutzerverhalten (nicht die eigentlichen Inhalte der übermittelten Daten!) werden ausgewertet und damit auch Profile erstellt. Denn nur so ist es möglich, anormales Benutzerverhalten und somit mögliche Angriffe rechtzeitig festzustellen. Die Auswertung von spezifischem Benutzerverhalten kann die Beurteilung wesentlicher Aspekte einer Persönlichkeit erlauben, weshalb davon auszugehen ist, dass mit IDS auch **Persönlichkeitsprofile** erstellt werden oder erstellt werden können.

Die eigentlichen Inhalte, welche über das Internet geschickt werden, interessieren im Rahmen von Intrusion Detection weniger, weshalb es wohl mittels IDS-Systemen nicht zur Sammlung von **besonders schützenswerten Personendaten** kommt.

Trotzdem muss hier festgehalten werden, dass auch beim reinen **Aufzeichnen von Verkehrsdaten** (wer hat wann mit gemailt, wer hat wann auf welche Homepage zugegriffen etc.) interessante Rückschlüsse gezogen werden können. Ohne dass man den genauen Inhalt weiss, wird man mehr oder weniger sichere Rückschlüsse mit besonders schützenswertem Inhalt oder mit Persönlichkeitsprofilaspekten ziehen können.

Der Einsatz von IDS-Systemen ist demnach unter dem Aspekt des Datenschutzgesetzes zu überprüfen

4.2 Grundsätze der Datenbearbeitung

Entsprechend dem Grundsatz der **informationellen Selbstbestimmung** muss jede Datenbearbeitung (sowohl in der Schweiz als auch der EU und den Rechtsordnungen von Deutschland und Österreich) kumulativ **rechtmässig**, **verhältnismässig** und **zweckmässig** sein (Art. 4 DSG CH, Art. 6 und 7 der EU-Datenschutzrichtlinie 95/46). Entspricht die Datenbearbeitung nicht diesen Anforderungen, wird die Datenschutzgesetzgebung verletzt. Die betroffene Person hat dann ein Recht auf **Wiederherstellung des gesetzeskonformen Zustandes** und gegebenenfalls Anspruch auf **Schadenersatz**.

Beim Einsatz eines IDS sollten die Benutzer darüber informiert werden, dass im Rahmen von Detectionsmassnahmen Benutzerprofile erstellt werden oder erstellt werden könnten. Dies ist vor allem darum wichtig, weil sich die Benutzer dessen nicht bewusst sind und man mit einer vorgängigen Information sicherstellt, dass der informationellen Selbstbestimmung nachgelebt wird, d.h. der **Benutzer weiss, worauf er sich einlässt.**

Welche **Auswertungen** aus den Daten gezogen werden dürfen, orientiert sich am Zweck, nämlich hier konkret der Detection von Angriffen. Dasselbe betrifft die Frage, wie lange die entsprechenden **Daten aufbewahrt** werden sollen, nämlich nur so lange wie unbedingt notwendig. Wie oben ausgeführt, werden Informationen, die das System als Attacken qualifiziert, auf Discs kopiert, damit sie nachfolgend vom ID-Administrator überprüft werden können. Im Sinne der Datenschutzregelungen sollte diese Überprüfung so schnell wie möglich, sicher innerhalb von 24 Stunden, erfolgen. Dies sollte bei normalen Arbeitszeiten eines ID-Administrators möglich sein. Grosse Unternehmungen fordern sogar die Anwesenheit von ID-Administratoren rund um die Uhr (Peter James Thomas, Das Datenschutzgesetz im Privatbereich, Zürich 1994; Schweizer Alex, Data Mining Data Warehousing, Datenschutzrechtliche Orientierungshilfen für Privatunternehmen, Zürich 1999).

Die Datenschutzgesetzgebungen ermöglichen jeder Person, vom Inhaber einer Datensammlung **Auskunft** darüber zu verlangen, ob Daten über sie bearbeitet werden (Art. 8 DSG CH, Art. 12 der EU-Datenschutzrichtlinie 95/46). Wird ein solches Auskunftsrecht wahrgenommen, ist es wichtig, auch die IDS-Daten im Rahmen einer vollständigen Auskunft offen zu legen.

Falls für den Betrieb der IT oder für einzelne Teile davon ein **Outsourcing** betrieben wird, sind, wie immer, die entsprechenden Vorschriften betreffend Datenbearbeitung, Auskunftspflicht etc. auch dieser Unternehmung zu überbinden (Brändli Thomas, Outsourcing, Vertrags-, Arbeits- und Bankrecht, Bern 2001).

4.3 Datenschutz der Internetbenutzer

Da mit IDS unter dem Fokus der sofortigen Erkennung von Hackingattacken, dem Einschleusen von Malwareviren etc., sämtlicher Netzverkehr überwacht wird, ist das konkrete Datenschutzbedürfnis jeglicher Netzwerkbenutzer zu überprüfen. Auf die konkreten spezifischen Fragen der Arbeitnehmer wird im folgenden Abschnitt eingegangen.

Wie oben schon kurz angeführt, kann man aus rechtlicher Sicht in guten Treuen den Standpunkt vertreten, der Einsatz von ID unter dem konkreten technischen Fokus entspreche den **Pflichten des Systembetreibers** und es handle sich folglich auf jeden Fall um eine **zweckmässige und verhältnismässige Datenbearbeitung**. Mehr noch, wer sich im Internet und Intranet bewege, wisse um die technischen Dimensionen des Einsatzes von Spamfiltern, IDS und der grundsätzlichen Aufzeichnung von Logdateien. Am einfachsten ist es auch hier, wenn die Tatsache des Einsatzes eines IDS und die Art und Weise des Umganges damit den Netzwerkbenutzern beispielsweise auf einer Homepage, in AGB's etc. mitgeteilt werden kann, womit je nach Ausgestaltung sogar deren Zustimmung erwirkt werden kann.

Im Sinne der vom Gesetz geforderten Zweckmässigkeit und Verhältnismässigkeit einerseits und der damit verbundenen Forderung nach Datensparsamkeit (ein wesentlicher Aspekt der Verhältnismässigkeit) andererseits, ist es dem Betreiber eines IDS zu empfehlen, die Art und Weise der konkreten Datenbearbeitung zu **dokumentieren**. Dies auch, um bei Vorliegen möglicher Klagen wegen Datenschutzverletzung die eigene Position und die vorgenommenen Abklärungen beheben zu können.

Dies hat konkrete organisatorische Konsequenzen, es muss nämlich ein entsprechendes **Organisationsreglement** geführt, Änderungen nachgeführt und spezifisch vorgenommene **erweiterte Auswertungen protokolliert und begründet** werden.

Ein **Spezialfall** ist das Vorliegen von **False Positive.** Hier werden nämlich erweiterte Datenbearbeitungen vorgenommen, die fälschlicherweise vom System angeregt werden. Die Verhältnismässigkeit und Zweckmässigkeit begründet sich im geplanten und konsequent umgesetzten zielgerichteten Einsatz des IDS. Ein False Positive und dessen Bearbeitung als solche begründen folglich noch nicht eine Datenschutzverletzung. Ergeben sich aber False Positives, weil das **IDS** als solches **unsorgfältig aufgesetzt** wurde, oder werden aufgrund eines festgestellten False Positives nicht unverzüglich sämtliche möglichen Korrekturen am IDS-Einsatz vorgenommen, fehlt in diesen Punkten die Zweckmässigkeit und Verhältnismässigkeit, weil eben falsche und somit unrechtmässige Resultate generiert werden.

Ein False Positive gilt als **falsches Personendatum**, ist somit so schnell wie möglich zu berichtigen resp. im Sinne der Verhältnismässigkeit und Zweckmässigkeit beim IDS-Einsatz zu **löschen**.

4.4 Arbeitnehmerschutz

Überwachungs- und Kontrollsysteme, die das **Verhalten der Arbeitnehmer** am Arbeitsplatz **überwachen**, sind gesetzlich grundsätzlich **nicht zulässig**. Sind Überwachungs- oder Kontrollsysteme aus anderen Gründen erforderlich, so sind sie so zu gestalten und anzuordnen, dass die Gesundheit, Bewegungsfreiheit, kurz der Persönlichkeitsschutz der Arbeitnehmer, dadurch nicht beeinträchtigt wird (vgl. dazu insbesondere CH Arbeitsgesetz Verordnung Nr. 3, Art. 26 ArGV 3; Art. 7b und 8 II b der EU-

Datenschutzrichtlinie 95/46/EG; D Datenschutzgesetzgebung insbesondere § 12, 14, 28 BDSG; A insbesondere § 96 ArbVG). Gestattet sind permanente anonymisierte Auswertungen der Protokollierungen, um zu überprüfen, ob das Nutzungsreglement eingehalten wird. Solche Auswertungen dienen dazu, Beweise zu erheben, um Missbräuche sanktionieren zu können, die durch die technischen Schutzmassnahmen nicht verhindert werden konnten (z.B. Zugriffe auf Internetseiten, die nicht auf die Sperrliste der Firewall figurieren; vgl. dazu Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz des Eidgenössischen Datenschutzbeauftragten, www.edsb.ch).

Intrusion Detection Systeme sammeln Netzwerkinformationen und analysieren diese nach Mustern von Angriffen und ungewöhnlichen Aktivitäten, weshalb auch Rückschlüsse auf das Verhalten konkreter Benutzer gezogen werden. Das Ziel des Einsatzes von IDS ist aber **nicht** die **Verhaltenskontrolle** der Mitarbeitenden als solche, sondern die Detection von unzulässigen Angriffen auf das IT-System. Die Intrusion Detection Systeme sind demnach so zu gestalten und anzuordnen, dass sie nicht zur reinen, persönlichkeitsverletzenden Verhaltenskontrolle missbräuchlich eingesetzt werden. Dies kann insbesondere dadurch erreicht werden, dass die **Mitarbeitenden** über Art und Zweck der Kontrolle **informiert** werden, das **Management** die **Verantwortung** für Art und konkreten Inhalt der Überprüfung übernimmt. Die **regelmässige externe Revision** (Audit) sollte zudem mit der Überprüfung der Einhaltung der Gesetzmässigkeit beauftragt werden. Zudem sind bestehende Arbeitnehmervertretungen wie Betriebskommissionen zu informieren und ins Controlling angemessen einzubinden.

Auf der anderen Seite kann der Einsatz eines IDS im Sinne der Fürsorgepflicht des Arbeitgebers für den Arbeitnehmer direkt gefordert sein. Zu denken ist beispielsweise, dass das Arbeitsklima durch Störungen auf dem Netz grundsätzlich beeinträchtigt werden kann, dass für das Einschleusen von Viren der Verdacht fälschlicherweise auf Mitarbeitende fallen könnte, bis hin zu peer-to-peer-Problemen.

Je nach Tätigkeitsgebiet und Branche einer Unternehmung, ist der Einsatz eines IDS also nicht nur im Sinne der allgemeinen Informatiksicherheit, sondern auch des Arbeitnehmerschutzes notwendig.

5. Straf- und Telekommunikationsrecht

Um gegen den Angreifer in rechtlich beweisbarer Form etwas unternehmen zu können, müssen die Anforderungen der **Forensic** berücksichtigt werden; dazu zählt die Frage, ob und in welcher Form elektronische Urkunden als Beweise dienen. Dies betrifft sowohl den Bereich des Strafrechts als auch des zivilen Haftpflichtrechts (Aepli Michael, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Zürich 2004).

Je nachdem, wie das IDS technisch aufgesetzt wird, kann es die Anforderungen der Forensic erfüllen. Für den Richter relevant ist dabei vor allem die **Aussagekraft dieses Beweismittels,** d.h. dass in technischer und organisatorischer Hinsicht belegt werden kann, dass die aufgelegten elektronischen Daten für Beweiszwecke tatsächlich geeignet und bestimmt sind. Wichtig ist dabei der Nachweis, dass sie echt, d.h. nicht verfälscht, verändert oder abgeändert wurden. Aus prozessualer Sicht (Zivil- oder Strafprozessrecht) sind elektronische Urkunden schon lange als sogenannte Augenscheinobjekte zugelassen.

Je nach Landesrecht überbindet das **Telekommunikationsrecht** dem Betreiber von Internetdiensten zusätzlich gewisse Pflichten betreffend die Aufbewahrung von Benutzerdaten. Beispielsweise müssen in der Schweiz Fernmeldedienstanbieter die Verkehrs- und Rechnungsdaten während sechs Monaten aufbewahren (Art. 15 Abs. 3 BÜPF; Hansjakob Thomas, BÜPF/VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2002, S. 275 f.).
Als Fernmeldedienstanbieter zählen dabei Provider, welche fernmeldetechnische Übertragung von Informationen für Dritte (d.h. nicht für Mutter- oder Tochtergesellschaften) erbringen.

6. Corporate Governance

6.1 Anforderungen der Corporate Governance

Unter Corporate Governance versteht man das Verhältnis zwischen den Aktionären, also den Eigentümern einer Gesellschaft, dem Verwaltungsrat und der Geschäftsleitung. In diesem Sinne geht es um grundlegende Verhaltenspflichten im Bereich Organisation und Führung mit dem Ziel der Optimierung und Kontrolle der Organisation des Unternehmens (Marti Mario, Corporate Governance in öffentlich beherrschten Unternehmen, in Jusletter 13. Mai 2002).

Die OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) hat dazu so genannte OECD-Grundsätze der Corporate Governance ausgearbeitet. Diese bieten Orientierungshilfen für Gesetzes- und Regulierungsinitiativen in OECD-Mitglieds- wie auch Nichtmitgliedsländern. Sie sind in fünf Kapitel gegliedert; es geht im Wesentlichen um:

1. die Rechte der Aktionäre, insbesondere um Informations-, Wahl- und Mitwirkungsrechte;

2. die gerechte Behandlung der Aktionäre, insbesondere um die Gleichbehandlung innerhalb einer Aktionärskategorie und das Verbot des Insiderhandels;

3. die Rechte der Stakeholder wie Arbeitnehmer, Kreditgeber oder die öffentliche Hand und die aktive Zusammenarbeit der Unternehmen mit den Stakeholdern;

4. die Rechnungslegung und Offenlegung; dabei geht es um die rechtzeitige und sorgfältige Vermittlung wesentlicher und relevanter Informationen betreffend die finanzielle Situation, die Ertragslage, die Eigentumsverhältnisse, aber auch um die Information über die zentralen Grundsätze der Leitung der Gesellschaft, die Unternehmensziele, voraussehbare Risiken, die Struktur, die Unternehmenspolitik etc.;

5. die Verantwortlichkeit des Verwaltungsrates. Ziel dabei ist, eine professionelle strategische Führung der Unternehmung und somit auch eine effiziente Überwachung der operativen Geschäftsleitung sicherzustellen. Deshalb sind eine rechtzeitige korrekte Information, die Befähigung (fachliche Kompetenz), die Respektierung von Gesetzen und die faire Behandlung der Aktionäre zwingend.

Die von der OECD formulierten Anforderungen lassen sich aber mehrheitlich problemlos auch aus den geltenden Rechtsbestimmungen (z.B. im Gesellschaftsrecht oder Buchführungsrecht) ableiten.

Auch das als Reaktion auf den Enron-Skandal durch die USA erlassene Gesetz, der **Sarbanes Oxley Act**, kodifiziert strenge Corporate Governance Anforderungen. Dazu zählt die Forderung der Unabhängigkeit der Revisionsstelle und damit verbunden die regelmässige Auswechslung der Revisionsgesellschaft sowie der eindeutige Nachweis unternehmerischer Handlungen auf konkrete ausführende Personen.

Zur professionellen Führung einer Unternehmung und damit verbunden der Sicherung korrekter Information zählt zweifelsohne auch die Verantwortung für die IT-Infrastruktur und somit deren Überwachung mittels einem IDS.

6.2 Elektronische Buchführung und Archivierung

Die Buchführungs- und Aufbewahrungsvorschriften des OR (Art. 957 ff.) und die darauf abgestützte Geschäftsbücherverordnung verlangen grundsätzlich 10 Jahre Aufbewahrung der Buchführungsdaten und der dazugehörenden beweissichere Korrespondenz respektive Belege (auch in Deutschland gilt als Faustregel eine zehnjährige Aufbewahrungsfrist, § 257 HGB; in Österreich gilt grundsätzlich eine siebenjährige Aufbewahrungsfrist, § 189 HGB). Dies impliziert, dass sowohl software- als auch hardwaretechnisch diese **Daten unverfälschbar aufbewahrt, aber auch jederzeit lesbar gemacht werden müssen.**

Sehr viele Dokumente werden heute nur noch elektronisch erstellt oder nach Möglichkeit wenigstens in elektronische Form zur Archivierung überführt. Dabei ist es sehr wichtig, dass die elektronische Form urkundengetreu ist und im Zweifelsfall nachgewiesen werden kann, dass sie nicht abgeändert wurde. Auch muss sie selbst bei Wechsel von IT-Tools (Konvertierung) ihre Urkunden und Beweisqualität behalten. Dasselbe gilt, falls sicherheitsbezeugende Elemente wie Signaturen, Algorithmen etc. ungültig werden.

IDS ist sicher ein Instrument, um **mögliche Angriffe und Manipulationen** an solchen Urkunden und Daten grundsätzlich **zu verhindern** oder wenigstens im Ansatz zu verhindern.

6.3 Selbstregulierungen

Auch im Bereich der Selbstregulierungen hat sich im Sinne des Corporate Governance-Geistes einiges getan. Speziell zu erwähnen ist dabei das **Basel II-Abkommen**, in welchem sich die Banken sämtlicher Industrienationen verpflichtet haben, sich freiwillig strengen Kriterien in Bezug auf die Kreditvergabe, den eigenen Finanzierungsgrad und die eindeutige Zuordnung und Nachprüfbarkeit von Geschäftshandlungen auf und zu Personen zu unterwerfen.

Auch die vielen Qualitätszertifikate und Labels, die von Unternehmungen verwendet werden, zählen zu den Selbstregulierungen, denen sich viele freiwillig unterwerfen.

Die zweifelsfreie **eindeutige Zuordnung und Nachprüfbarkeit von Geschäftshandlungen** ist nur möglich, wenn das IT-System verlässlich läuft, sich darin keine Viren befinden, nicht gehackt wurde etc. Zur Erreichung dieser Selbstregulierungsanforderungen ist deshalb der adäquate Einsatz eines IDS sinnvoll.

6.4 Rechtssicherheit

Das Sicherstellen von **Rechtssicherheit,** d.h. der Ausschluss von Prozess- und Schadenrisiken wegen schlecht gestalteten oder ungeklärten Rechtssituationen oder Rechtsbeziehungen, zählt in der **Informationsgesellschaft** in steigendem Mass zum Bedürfnis von Unternehmungen und somit zu einem wesentlichen Teil des Riskmanagements. Klagen wegen Urheberrechtsverletzungen, Datenschutzverletzungen, Markenverletzungen, unzulässigem Gebrauch von Domainnamen, Versenden unzulässiger Inhalte übers Internet (Computerkriminalität), unzulänglicher Archivierung elektronischer Dokumente etc. sind heute ernst zu nehmende Bedrohungen. Sehr viele dieser Bedrohungen lassen sich durch rechtzeitige Abklärung und korrekte Gestaltung von Beziehungen oder unternehmerischen Prozesse (z.B. Datenarchivierung) mit Weisungen und Policen vermeiden. In diesem Sinne sind die Spezialisten von Legal Compliance sowie Rechtsanwältinnen und Rechtsanwälte nicht nur, wie traditionell gehandhabt, erst nach Schadeneintritt beizuziehen, sondern sinnvollerweise schon bei der Umsetzung eines sinnvollen Riskmanagement-Prozesses.

Die Detection und Repression von Angriffen auf die IT-Ressourcen bilden einen wesentlichen Beitrag zur Einhaltung von Rechtssicherheit.

7. Corporate Governance und IDS: Zielkonflikte

Zur sorgfältigen und umsichtigen Unternehmensführung zählt ein Maximum an Informatik- und Rechtssicherheit. Sowohl die **Detection** als auch die damit verbundenen notwendigen Handlungen sind unbestrittenermassen Bestandteil der **unternehmerischen Verantwortungen** des Managements. Denn zu den unternehmerischen Pflichten gehört es, Risiken maximal zu vermeiden und die Einhaltung von gesetzlichen und selbstregulierenden Normen (Compliance) zu kontrollieren. Zu diesen gesetzlichen Pflichten gehört selbstverständlich auch die Einhaltung von Datenschutz; dies ist unbestritten eine Managementverantwortung.

Die Einhaltung von Persönlichkeits- und Datenschutz verlangt einen sehr **sparsamen Umgang mit Datenbearbeitung;** für den privatrechtlichen Bereich gilt hier: Je weniger, desto besser, nur so viel wie unbedingt nötig! Auf der anderen Seite sind die Unternehmungen gehalten, möglichst sämtliche relevanten Daten nachweisbar zu archivieren, um compliant zu sein.

Der Einsatz von IDS betrifft grundsätzlich sämtlichen Datenverkehr. Gegenüber den Mitarbeitern kann man den Datenschutzanforderungen gerecht werden, indem man sie über den IDS-Einsatz informiert und deren **Einwilligung** für die damit verbundene Datenbearbeitung einholt. Wer von aussen, wie z.B. Kunden, Kreditgeber, Mitbewerber etc., Daten übermittelt, wird über diese Bearbeitungsform wohl kaum informiert sein, geschweige denn die Möglichkeit gehabt haben, seine Einwilligung dazu zu geben. Hier wäre mindestens ein Hinweis auf der Website der Unternehmung zu empfehlen.

Unter dem Fokus, für welchen IDS eingesetzt wird, könnte auch geschlossen werden, sei eine zweckmässige und verhältnismässige Datenbearbeitung im Rahmen der **Informatiksicherheitsverantwortung** des Systembetreibers korrekt. Davon müsse ein Benutzer ausgehen, da ja auch bekanntlich sämtliche Logdaten für eine gewisse Zeit aufbewahrt werden.

Datenbearbeitungen, insbesondere Aufbewahrungen, sollten nur von einer bestimmten Person vorgenommen werden, welche auch einer internen absoluten **Geheimhaltung** unterliegt. Dies hilft mit, die Zweckmässigkeit der Datenbearbeitung zu gewährleisten. Für weitergehenden Zugriff und Bearbeitungsformen sollte man die Daten nach Möglichkeit anonymisieren.

Interessant wären sicher auch technische Lösungen, die diese rechtlichen Anforderungen unterstützen könnten. Bei der Konzeption des IDS-Systems und bei der Planung des konkreten Einsatzes eines IDS sind auch die verschiedenen normativen (Law und Softlaw) und daraus folgenden organisatorischen Anforderungen zu berücksichtigen und bei der Umsetzung einfliessen zu lassen. Dies hat möglicherweise zur Folge, dass das IDS datenhygienisch eingesetzt werden muss und ergänzend noch weitere organisatorische und rechtliche Vorkehrungen (beispielsweise vertragliche Vereinbarungen) notwendig sind, um der **Compliance** gerecht zu werden.

8. Schlussfolgerungen

Der Einsatz von IDS als ein Mittel zur Feststellung von Hackingattacken und dem Eindringen von Malwareviren etc. wird faktisch immer wichtiger und kann unter dem Aspekt der IT-Governance zwingend sein. Den berechtigten Interessen der Internet-Benutzer auf informationelle Selbstbestimmung muss aber unbedingt Rechnung getragen werden. Deshalb sind vor der konkreten Konzipierung und dem Einsatz eines IDS die Anforderungen des Datenschutzes zu berücksichtigen und bei der Umsetzung miteinzubeziehen. Dies erfolgt insbesondere in

- der Festlegung der datenschutzrechtlichen Fragen beim konkreten Einsatz
- der Aufzeichnung, welche Vorkehrungen man einsetzt, dass keine Datenschutzverletzungen eintreten.

Die Vorkehrungen können, je nach Situation, verschieden aussehen. Es kann sich dabei handeln um

- eine Information der Arbeitnehmer über Art und Weise des IDS-Einsatzes
- einen Hinweis für Drittbenutzer auf einer Homepage
- einen dauernden zweck- und verhältnismässigen Einsatz des IDS
- die Protokollierung der Änderungen am System und des Vorgehens bei einem False Positive.

Literatur:

- Aepli Michael, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Zürich 2004.

- Baeriswyl Bruno / Rudin Beat, Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich 2002.

- Brändli Thomas, Outsourcing, Vertrags-, Arbeits- und Bankrecht, Bern 2001.

- Fuhrberg Kai / Häger Dirk / Wolf Stefan, Internet–Sicherheit, 3. Auflage, München 2001.

- Hansjakob Thomas, BÜPF/VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2002.

- Kilian Wolfgang / Wiebe Andreas, Data Security in Computer Networks and Legal Problems, Beiträge zur juristischen Informatik, Band 17, Darmstadt 1992.

- Marti Mario, Corporate Governance in öffentlich beherrschten Unternehmen, in Jusletter 13. Mai 2002.

- Northcutt Stephen / Novak Judy, Intrusion Detection, Spurensuche im Internet, Deutsche Ausgabe, Bonn 2001.

- Peter James Thomas, Das Datenschutzgesetz im Privatbereich, Zürich 1994

- Schweizer Alex, Data Mining Data Warehousing, Datenschutzrechtliche Orientierungshilfen für Privatunternehmen, Zürich 1999.

- Wildhaber Bruno, Informationssicherheit, Rechtliche Grundlagen und Anforderungen an die Praxis, Zürich 1993.

- Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz des Eidgenössischen Datenschutzbeauftragten für öffentliche Verwaltungen und Privatwirtschaft, 2003.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH). Sie ist ferner Professorin für Informatikrecht an der Fachhochschule und leitet den Diplomstudiengang Wirtschaftsinformatik an der Hochschule für Wirtschaft HSW Luzern der Fachhochschule Zentralschweiz. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig. Informieren Sie sich unter www.hsw.fhz.ch

30.3.05