

IT-Sicherheit in Netzwerken – Praktische Aufgaben 2

IT-Sicherheit kann nur gewährleistet werden, wenn sowohl technische Realisierungen und gesellschaftliche Konventionen miteinander harmonieren. Gesetze werden gemacht, um die getroffenen Übereinkünfte einerseits schriftlich zu fixieren (objektives Recht) und andererseits die ableitbaren Befugnisse Einzelner zu regeln (subjektives Recht). Im Zusammenhang mit Rechtsproblemen, die durch den Einsatz von neueren Technologien, wie auch dem Internet und dem Web, entstehen können, muss festgehalten werden, dass es kein so genanntes „Internet-Recht“ gibt. Die resultierenden Rechtsprobleme haben Einfluss auf die unterschiedlichsten Rechtsgebiete, wie elektronischer Geschäftsverkehr, Datenschutz und Vorratsdatenspeicherung oder auch Markenrecht.

Im Folgenden werden zwei Rechtsfelder beispielhaft betrachtet, die ebenfalls eng mit Fragen der IT-Sicherheit verknüpft sind:

- Sicherheit durch Videoüberwachung und
- Sicherheit durch digitale Signaturen (IuKDG, Signaturgesetz).

Somit besteht das zweite Praktikum aus zwei Teilen

- A. Diskussion der Frage: Was leistet Videoüberwachung?
- B. Nutzung von digitalen Signaturen, um digitale Dokumente zu signieren

Nach der Durchführung des Praktikums kennen Sie die Vor- und Nachteile von Sicherheitssystemen, die auf Überwachung und Vernetzung von Videokameras setzen. Die Diskussion erfolgt an einem konkreten Beispiel. Sie kennen die Rechtsgebiete, die zu berücksichtigen sind, wenn ein Videoüberwachungssystem zu implementieren ist. Sie können einschätzen, wann die Implementierung eines Netzes von Videokameras mehr Sicherheit bieten kann.

Nach Bearbeitung des zweiten Teils können Sie elektronische Dokumente signieren und damit die Echtheit der Dokumente unter Nutzung von freiverfügbarer Software nachweisen.

Teil A: Diskussion – Was leistet Videoüberwachung?

Durch den Fortschritt der technischen Entwicklung und immer geringer werdenden Preisen werden an vielen Stellen Videokameras installiert. Tankstellen, Tiefgaragen, Bahnhöfe, Innenstädte und Kaufhäuser und viele weitere Orte werden überwacht.

1. Nennen Sie mindestens drei weitere Orte, an denen Ihnen Videokameras aufgefallen sind.
2. An einem Eingangsbereich einer Firma ist eine Videokamera installiert. Welche Formen von Kontrollen sind hier erwünscht und warum? Listen Sie insbesondere die Ziele auf, die mit einer solchen Videoüberwachung verbunden sein könnten.
3. Überlegen Sie sich mindestens zwei weitere Anwendungsszenarien, in denen Videokameras zum Einsatz kommen und beschreiben Sie diese in einem Use Case und besser noch einem Sequenz-Diagramm. Als Grundlage zur Beschreibung von diesen Anwendungsszenarien können Sie auch Ihre Beispiele aus Aufgabe 1 nehmen. Beschreiben Sie die Schutzziele und Schwachstellen, die sich ggf. aus

- den gewählten Anwendungsszenarien (insbesondere Sequenzdiagrammen) ableiten lassen.
4. Verallgemeinern Sie die bisher ermittelten konkreten Schutzziele. Finden Sie Begriffe, die diese Schutzziele möglichst allgemein beschreiben lassen.
 5. Für den Begriff Videoüberwachung gibt es keine einheitliche Definition.
 - a. Recherchieren Sie zuerst, wie der Begriff „Überwachung“ aufgefasst werden kann.
 - b. Bringen Sie Ihre Recherche-Ergebnisse zum Begriff „Überwachung“ in Verbindung mit den technischen Möglichkeiten, die sich aus der Nutzung einer und/oder mehrerer Videokameras ergeben. Ziehen Sie Ihre eigenen Schlüsse: Was kann also Videoüberwachung leisten? Was kann Videoüberwachung nicht leisten? (Hinweis: Welche Formen von Informationen haben Sie nicht, wenn Sie ausschließlich Bilddaten betrachten?)
 6. Welche (Bürger-)Rechte werden ggf. durch Videoüberwachung eingeschränkt? Listen Sie diese auf und diskutieren Sie diese möglicherweise kritischen Punkte in der Gruppe.

Nachdem Sie sich ausführlich mit den Rahmenbedingungen von Videoüberwachung beschäftigt haben, sollen nun die tatsächliche Anwendung einer Videoüberwachungsanlage studiert werden. Dazu gehen wir auf das Gelände der Hochschule. *Sie erhalten eine Kopie einer vereinfachten Karte des Hochschulgeländes. Diese Karte mit Ihren Einträgen ist nach Bearbeitung und gemeinsamer Auswertung Ihrer Ergebnisse wieder HEUTE (21.11.2008) abzugeben.*

7. Auf dieser Karte zeichnen Sie, bitte, die gefundenen Videokameras ein, die Sie bei einem 30-minütigen Spaziergang über das Gelände finden.
8. Versuchen Sie beim Einzeichnen der Videokameras, den Beobachtungswinkel einer jeden Kamera einzuschätzen. Beachten Sie einige Kameras sind schwenkbar gelagert. Zeichnen Sie den möglichen Beobachtungsradius in die Karte mit ein.
9. Nachdem Sie Ihre Erhebung gemacht haben, werden wir die Karten gemeinsam auswerten. – Welche Schlüsse lassen sich ziehen?

Teil B: Nutzung von digitalen Signaturen

Eine digitale Signatur kann als elektronische Unterschrift aufgefasst werden. Mit einer persönlichen Unterschrift wird von uns auf Papier in der Regel bestätigt, dass die gemachten Angaben korrekt sind. Denken Sie daran, dass Sie üblicherweise Ihren Lebenslauf in einer Bewerbung unterschreiben oder dass Sie einen Betrag auf einer Rechnung mit Ihrer Unterschrift quittieren. Eine Unterschrift wie auch später eine digitale Signatur sind Prüfmerkmale.

Das so genannte Signaturengesetz regelt den Gebrauch von digitalen Unterschriften und Verschlüsselungsverfahren im elektronischen Nachrichtenverkehr. Typischerweise werden digitale Signaturen im Emailwechsel verwendet. Aber auch andere digitale Dokumente können signiert werden. Im Folgenden findet sich ein Beispiel eines signierten Textes, Abbildung 1. Auch wenn digitale Signaturen und auch Verschlüsselungsverfahren sich in Teilen gleicher Techniken bemitteln, dient die

digitale Signatur nur zum Signieren und damit der Bestätigung der Echtheit eines digitalen Dokuments¹.

Abbildung 1: Text mit digitaler Signatur

```
-----BEGIN PGP SIGNED MESSAGE-----  
  
Hash: SHA1  
  
Das ist ein Beispiel eines signierten Textes.  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.8 (Darwin)  
  
iJwEAQECAAYFAkkizcUACgkQiqtiYTlU4DfWUQP8CPqpMIjMamQy6DIH6dCmFC  
F4  
8SK2A4PEJSfJqle5LcRcRFZQd0BilCBitGlInB5qCI5K+Kj/Z3uSOlwtE+38YO  
pA  
cXROACNxe4Jmar8bih29neqtIILFJYAfGvyMui+Qp8eTyKs+cXc1Vm6DRZYKxH  
BV  
oC0Abr93bhftrTkiHTI=  
=nTBs  
-----END PGP SIGNATURE-----
```

Dieser Text besteht aus dem tatsächlichen Inhalt „Das ist ein Beispiel eines signierten Textes.“ als auch der einer digitalen Signatur. Die digitale Signatur ist entstanden durch die Verwendung eines asymmetrischen (Verschlüsselungs-)Verfahrens basierend auf dem Programm PGP (pretty good privacy). Natürlich gibt es auch andere (Verschlüsselungs- und Signierungs-)Programme. Dennoch kann PGP als Quasi-Standard angesehen werden.

Unter Nutzung von PGP sind jedem Teilnehmer, der signierte Texte verschickt, zwei so genannte Schlüssel zugeordnet: ein privater Schlüssel und ein öffentlicher Schlüssel. Mit dem privaten Schlüssel wird signiert (oder verschlüsselt). Mit dem öffentlichen Schlüssel kann die Echtheit des Textes durch jeden anderen Empfänger der Email oder des Textes überprüft werden.

Ihre Aufgabe ist es das Programm PGP zu installieren, Dokumente zu signieren und Ihren öffentlichen Schlüssel für andere Teilnehmer nutzbar zu machen.

Um PGP zum Signieren von Texten nutzen zu können, müssen Sie folgende Arbeitsschritte durchführen. Während der Installation und Anwendung sollten Sie auch noch ein paar Fragen beantworten, um ein besseres Verständnis für Vor- und Nachteile zu bekommen, die beim Gebrauch von digitalen Signaturen entstehen können.

1. Gehen Sie auf die Webseite <http://www.pgpi.org/>
Das PGP Programm, das Sie benötigen, finden Sie unter „the de-facto standard for email encryption“. Hier finden Sie die verschiedensten Versionen des PGP Programms für die unterschiedlichsten Betriebssysteme. Suchen Sie sich die führ

¹ Verschlüsselungsverfahren sind aufwendiger und werden später auch ausführlicher behandelt.

- Ihr Betriebssystem passende Version heraus und laden Sie das Programm herunter.
2. Installieren Sie das Programm (durch Lesen der gegebenen Dokumentation).
 3. Auf welcher Methode basiert üblicher Weise das Verfahren für die Erstellung einer digitalen Signatur? Hinweis: Schauen Sie ggf. in die Dokumentation von PGP.
 4. Welche Garantien neben Echtheit einer Nachricht sollen mit einer digitalen Signatur noch gegeben werden. Finden Sie diese Eigenschaften heraus. Können diese immer mit einer digitalen Signatur garantiert werden? (Gibt es also Schwachstellen im Signaturgesetz?)
 5. Generieren Sie ein Schlüsselpaar (privater und öffentlicher Schlüssel).
 6. Finden Sie heraus, wie Sie sich Ihre Schlüssel zertifizieren lassen können.
 7. Führen Sie eine kostenlose Zertifizierung durch.
 - a. Welche Möglichkeiten gibt es für eine kostenlose Zertifizierung?
 - b. Mit wem Tauschen Sie also Schlüssel in welcher Form aus, bevor Sie irgendeine Nachricht signieren?
 - c. Wie machen Sie (dann) Ihren öffentlichen Schlüssel öffentlich? Und publizieren diesen Schlüssel auch!
 8. Schreiben Sie einen beliebigen Text und signieren Sie ihn mit zertifiziertem Schlüssel. (Hinweis: Überlegen Sie vorher welchen Schlüssel Sie wann benutzen.)
 9. Schicken Sie sich Ihre Texte gegenseitig zu und prüfen Sie die signierten Nachrichten.
 10. Schicken Sie sich Ihre Texte mit fehlerhaften Signaturen zu (z.B. durch Löschen einzelner Zeichen in der Signatur). – Was passiert bei der Überprüfung auf Echtheit der Dokumente? Welche Fehlermeldung erhalten Sie?