

Sicherheitstechnische Evaluierung des Verfahrens Ki-ON

**im Auftrag der
Redlink Mediendienste GmbH**

datenschutz nord GmbH

Oktober 2001

Sicherheitstechnische Evaluierung des Verfahrens Ki-ON

Die datenschutz nord GmbH hat im September/Oktober das Verfahren Ki-ON der Redlink Mediendienste GmbH evaluiert. Das Verfahren wurde auf der Basis einer allgemeinen Risikoanalyse anhand spezifischer Sicherheitsziele sowohl konzeptionell bewertet als auch einem praktischen Sicherheitstests unterzogen.

Die Evaluierung erfolgte im Auftrag der Redlink Mediendienste GmbH. Zur Durchführung der Evaluierung wurden vom Auftraggeber sämtliche benötigten Unterlagen sowie ein Testzugang zu Ki-ON zur Verfügung gestellt.

Die Ergebnisse dieser Evaluierung stellt der folgende Bericht ausführlich dar.

Insgesamt hat sich bei der Evaluierung herausgestellt, dass das Verfahren Ki-ON eine weitgehend sichere Plattform zur Verarbeitung sensibler personenbezogener Daten darstellt und den Sicherheitsanforderungen entspricht, die an dementsprechende Client-Server-Verfahren gestellt werden.

Die im Bericht empfohlenen Maßnahmen zur weiteren Verbesserung der Sicherheit (vgl. Kap. 7 des Berichts) wurden von der Redlink Mediendienste GmbH konstruktiv aufgegriffen und – wie in der Anlage beschrieben – umgesetzt.

Bremerhaven, 31. Oktober 2001

datenschutz nord GmbH

Dr. Uwe Schläger (Geschäftsführer)

Inhalt

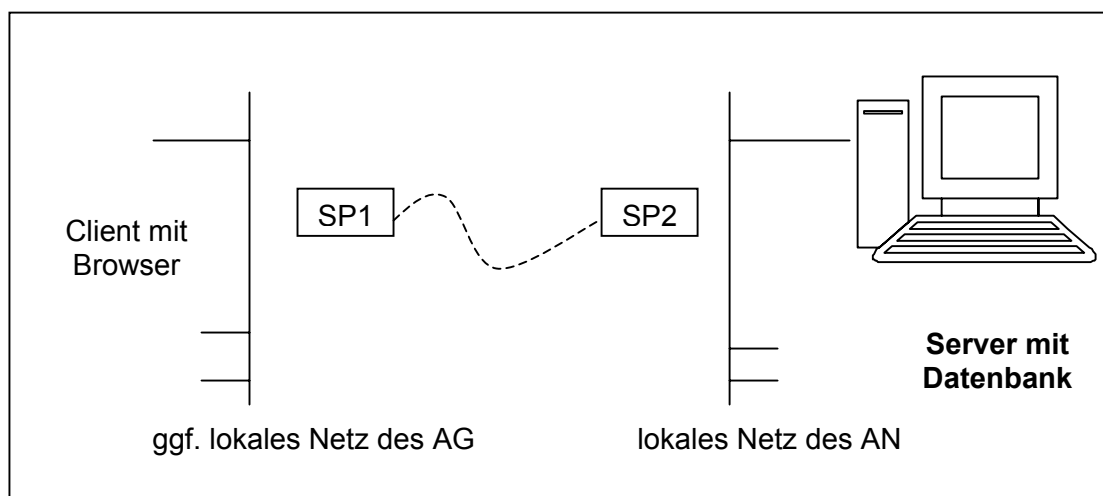
1	BESCHREIBUNG DES VERFAHRENS	1
2	VORGEHENSWEISE	1
3	RISIKOANALYSE	2
3.1	Vertraulichkeit	2
3.2	Integrität	4
3.3	Verfügbarkeit	5
3.4	Authentizität	6
4	SICHERHEITZIELE	7
4.1	Need-to-know-Prinzip	7
4.2	Geschlossene Benutzergruppe	8
4.3	Beweise statt Vertrauen	8
4.4	Robustheit	8
5	SICHERHEITSMECHANISMEN	8
5.1	Server	8
5.2	Firewall	10
5.3	Secure Sockets Layer (SSL)	11
5.4	Secure Shell (SSH)	13
5.5	Benutzerauthentisierung	13
5.6	Terminalauthentisierung	15
5.7	Zugriffschutz	16
5.8	Tripwire	17
6	ÜBERPRÜFUNG DER SICHERHEITSMECHANISMEN	18
6.1	Server	19
6.2	Firewall	21
6.3	Web-Server und SSL	21
6.4	SSH	23
6.5	Benutzerauthentisierung	24
6.6	Terminalauthentisierung	24
6.7	Zugriffschutz	25
7	ERGEBNISSE UND EMPFEHLUNGEN	25
A	VERFAHRENSÄNDERUNGEN	27
	LITERATUR	29

1 Beschreibung des Verfahrens

Beim Client-Server-Verfahren Ki-ON handelt es sich um ein System der Firma RedLink Mediendienste für Tageseinrichtungen für Kinder und Jugendliche. Gegenstand des Verfahrens ist die Verarbeitung und Verwaltung von vertraglich und gesetzlich festgelegten Daten, die die Kindertagesstätten in ihrer Funktion als Träger der Kinder- und Jugendhilfe sowie für eigene Zwecke erheben und verarbeiten. Dabei handelt es sich einerseits um personenbezogene Daten der betreuten Kinder bzw. deren Eltern und des beschäftigten Personals, andererseits um Organisation-, Planungs- und Statistikdaten ohne Personenbezug.

Die Firma Redlink Mediendienste betreibt hierfür ein zentrales System, auf das die Kindertagesstätten über das Internet mittels eines Standard-PC zugreifen können. Die Client-Seite dient dabei ausschließlich als Front-End, d.h. dort erfolgt lediglich die Datenein- und -ausgabe, jedoch keine Auswertung und keine Speicherung der Daten. Sämtliche auf Client-Seite verarbeiteten Daten werden daher über das Internet zwischen Kindertagesstätte und dem Server übertragen und liegen in dauerhafter Form nur dort vor. Die Kindertagesstätten sind im Rahmen des Auftragsverhältnisses in der Verwendung der Zugangstechnik, insbesondere Hardware, Browser, Betriebssystem, installierte Software und Art und Anbieter des Internet-Zugangs frei, solange bestimmte Mindestvoraussetzungen eingehalten werden.

Das Gesamtsystem stellt sich bei einer groben Betrachtungsweise wie folgt dar:



2 Vorgehensweise

Für die vorliegende Studie wurde folgendes Vorgehen gewählt: Ausgehend von einer allgemeinen Risikoanalyse, die anhand des beschriebenen Verfahrens auf konkrete Risiken abgebildet wird (Abschnitt 3), werden Sicherheitsziele formuliert, die zu erreichen sind (Abschnitt 4). Anschließend werden die Mechanismen, die in dem Verfahren Ki-ON implementiert wurden, benannt und auf Grundlage der entwickelten Ziele bewertet (Abschnitt 5).

Im Anschluss an diesen konzeptionellen Teil wird das Verfahren einer praktischen Überprüfung hinsichtlich der Sicherheitsmechanismen unterzogen (Abschnitt 6) und abschließend die erzielten Ergebnisse nochmals zusammengefasst (Abschnitt 7).

3 Risikoanalyse

Hinsichtlich der Risiken bei der Verarbeitung von Daten lassen sich verschiedene Aspekte unterscheiden:

- Vertraulichkeit, d.h. die Gefahr, dass die Daten Unberechtigten zugänglich werden
- Integrität, d.h. die Gefahr, dass die Daten verfälscht werden
- Verfügbarkeit, d.h. die Gefahr, dass die Daten nicht vollständig oder nicht rechtzeitig zur Verfügung stehen
- Authentizität, d.h. die Gefahr, dass die Daten nicht vom angegebenen Urheber stammen

Diese Risiken sind keine Ki-ON-spezifischen Schwachstellen, sondern Gefahrenpotentiale, die generell bei EDV-Einsatz zu berücksichtigen sind. Die Gewichtung der einzelnen Risiken hängt zum einen von der Art und Weise der Datenverarbeitung und Datenhaltung und zum anderen von der Art der verarbeiteten Daten selbst ab. Bei Daten etwa, die öffentlich zugänglich sind, z.B. die Preisliste eines Herstellers, wird der Vertraulichkeit keine, der Integrität jedoch wesentliche Bedeutung zukommen.

Im betrachteten Verfahren Ki-ON werden sensible personenbezogene und unternehmenskritische Daten verarbeitet, die sowohl aus den rechtlichen Anforderungen heraus als auch aus Eigeninteresse des AG möglichst geringen Risiken ausgesetzt sein müssen. Um dies mit geeigneten Maßnahmen erreichen zu können, sind die genannten abstrakten Gefährdungsbereiche auf konkrete Gefahren abzubilden. Diese können in den verschiedenen Teilen des oben skizzierten Gesamtsystems lokalisiert werden:

- Client (PC beim AG)
- lokale Netze (einschließlich Zugangstechnik zum Internet; kann auf Seite des AG auch entfallen)
- Internet (gesamte Datenstrecke außerhalb der Verfügungsgewalt des AG und des AN)
- Server (Rechner einschließlich eventueller Zusatzkomponenten wie Firewall beim AN)

3.1 Vertraulichkeit

Durch die unberechtigte Kenntnisnahme von Daten kann beträchtlicher Schaden entstehen, und die Rechte Betroffener können empfindlich verletzt werden. Ein solcher Missbrauch ist sowohl durch Interne als auch durch Externe möglich.

3.1.1 Client

Zwar werden bei Ki-ON Client-seitig keine Daten gespeichert, dennoch sind an diesem Punkt sämtliche Daten, die eingegeben oder abgerufen werden, verfügbar. Einem Angreifer, dem es gelingt, auf den Client zuzugreifen, während dieser benutzt wird, kann daher u.U. vertrauliche Daten zur Kenntnis nehmen. Ein solcher Angriff kann erfolgen, indem eine Zusatzsoftware (z.B. in Form eines sog. Trojanischen Pferds) auf dem Client installiert wird, die Daten z.B. für einen späteren Abruf aufzeichnet oder direkt über das Internet an den Angreifer sendet. Die Installation einer solchen Software kann auch über das Internet selbst erfolgen.

3.1.2 Lokale Netze

Auch außerhalb des offenen Internet kann die Vertraulichkeit gefährdet werden. Erfolgt der Zugang zum Verfahren Ki-ON beim AG in einem lokalen Netz, ist es bei der Verwendung gängiger Techniken (Ethernet mit Koaxialverkabelung oder mit Twisted-Pair-Verkabelung über einen lokalen Hub; doch auch geschwitze Netze sind gefährdet [Song 2000]) möglich, die Daten eines anderen Netzteilnehmers am eigenen Anschluss zur Kenntnis zu nehmen. Dies kann, je nach Aufteilung der Nutzungsberechtigungen innerhalb des AG, dazu führen, dass Daten durch Interne unberechtigt zur Kenntnis genommen werden. Entsprechendes gilt für das lokale Netz des AN.

3.1.3 Internet

Sämtliche Daten (Inhaltsdaten, Verbindungsdaten, Steuerungsdaten, Authentisierungsdaten) werden über das Internet zwischen Client und Server übertragen. Das Internet stellt zwar eine virtuelle Punkt-zu-Punkt-Verbindung zwischen den Endsystemen her, diese wird jedoch über eine Vielzahl von zwischengeschalteten Vermittlungsrechnern realisiert, die in technischer Hinsicht Zugriff auf die Daten haben. Diese Zwischenstationen werden fallweise und nach den Anforderungen des Netzverkehrs gewählt und liegen in der Verfügungsgewalt Dritter. Eine unberechtigte Kenntnisnahme der Daten während der Übertragung durch Externe kann daher nicht ausgeschlossen werden.

3.1.4 Server

Auf dem Server liegen sämtliche Daten aller angeschlossenen Kunden. Ein Zugriff auf diesen Datenbestand bedeutet daher das größtmögliche Risiko für die Vertraulichkeit. Zu unterscheiden ist hier zwischen internem und externem Missbrauch. Aus technischen Gründen ist es unvermeidbar, dass administrative Kräfte des AN sowie ggf. von diesem beauftragte Subunternehmer zur Gewährleistung des störungsfreien Betriebs die Möglichkeit haben, auf die Speichermedien zuzugreifen. Dies bedeutet jedoch nicht, dass damit die Berechtigung einhergeht, sämtliche dort gespeicherten Daten zur Kenntnis zu nehmen. Die Vertraulichkeit muss daher auch durch diese internen Kräfte gewährleistet werden.

Zum anderen kann es Externen gelingen, auf den Server und dort verfügbare Daten zuzugreifen, z.B. indem bestimmte technische Mängel der verwendeten Software ausgenutzt werden. Da der Server über das Internet erreichbar ist, kommen als Täter eine Vielzahl sehr versierter Angreifer (Hacker, Geheimdienste etc.) in Betracht. Ebenfalls stellt der Zugriff eines Kunden auf die Datenbestände eines anderen Kunden ein Risiko für die Vertraulichkeit dar.

3.2 Integrität

Integritätsverletzungen können grundsätzlich durch aktive Eingriffe von Angreifern oder durch technisches Versagen entstehen. Da letzteres Problem durch entsprechende technische Vorkehrungen weitgehend beherrscht wird, soll hier nur auf bewusste Verfälschungen eingegangen werden. In der Regel setzt dies die Möglichkeit der Kenntnisnahme der Originaldaten voraus, da nur auf diese Weise "sinnvolle" Veränderungen getätigt werden können.

3.2.1 Client

Eine Veränderung der Daten im Client ist im Ki-ON-Szenario kaum möglich. Da dort keine Datenspeicherung stattfindet, müssten die Daten während der kurzen Zeitspanne zwischen Empfang aus dem Netz und Darstellung auf dem Bildschirm bzw. zwischen Eingabe und Absenden verändert werden. Während dies nach entsprechender Manipulation des Client zwar prinzipiell möglich wäre (etwa durch Einfügen eines lokalen Proxies), wäre der Aufwand dafür vergleichsweise hoch und der "Nutzen" für einen Angreifer gering.

3.2.2 Lokale Netze

Ethernet-basierte lokale Netze verhindern aufgrund ihrer Funktionsweise eine Datenverfälschung durch andere Teilnehmer. Lediglich an vermittelnden zentralen Punkten (Switches, Router) oder Netzübergängen wäre eine inhaltliche Änderung der Daten möglich. Dies setzt jedoch eine vollständige Kontrolle des Geräts sowie dessen Umprogrammierung voraus.

3.2.3 Internet

Die im Internet verwendete Protokollfamilie TCP/IP stellt einfache Mechanismen zur Wahrung der Integrität der Daten zur Verfügung; diese zielen jedoch ausschließlich auf Veränderungen aufgrund technischer Fehler. Gezielte Änderungen unter Berücksichtigung dieser Mechanismen sind damit weder zu verhindern noch zu entdecken. Da, wie beschrieben, die Daten auf dem Weg vom Sender zum Empfänger über eine Vielzahl von Zwischenstationen laufen, sind daher inhaltliche Veränderungen an diesen Stellen möglich.

3.2.4 Server

Risiken für die Integrität beziehen sich auf dem Server vor allem auf die dort gespeicherten Daten. Hier muss wieder zwischen internen und externen Angreifern unterschieden werden. Administrative Kräfte mit Zugriff auf die Datenträger bzw. das verwendete Datenbanksystem sind technisch in der Lage, jedes Datum zu verändern. Dies gelingt in der Regel ohne beweiskräftige Spuren zu hinterlassen.

Externen Angreifern kann es unter Umständen ebenfalls gelingen, sich in diese Position zu begeben und damit Daten dauerhaft zu verändern. Ein solcher Angriff würde damit den gesamten Datenbestand in Frage stellen. Auch die Möglichkeit, die Daten eines anderen Kunden zu manipulieren, gehört in diese Kategorie.

3.3 Verfügbarkeit

Eine der Grundanforderungen an ein Datenverarbeitungssystem ist die umgehende und vollständige Zurverfügungstellung von Daten. Wie bei der Integrität kann diese sowohl durch technische Probleme als auch durch aktive Eingriffe beeinträchtigt werden. Da technische Ausfälle und Fehlfunktionen auf allen Ebenen (Hardware, Betriebssystem, Anwendungssoftware) vergleichsweise häufig sind, soll hier auf beide Aspekte eingegangen werden.

3.3.1 Client

Hinsichtlich der Verfügbarkeit stellt im Verfahren Ki-ON der Client eine weitgehend unproblematische Komponente dar. Da es sich um Standard-Geräte ohne spezielle Software handelt, lässt sich ein defektes Gerät problemlos ersetzen, sofern ein anderer PC zur Verfügung steht. Andernfalls kann, zumindest bei Software-Problemen, durch Neuinstallation ein operabler Zustand wieder hergestellt werden.

Gleichwohl kann es einem Angreifer aus dem Internet heraus gelingen, einen Client zu stören, z.B. abstürzen zu lassen. Während eine dauerhafte Beeinträchtigung dadurch nicht möglich ist, sind die Daten jeweils bis zum Neustart des Systems nicht verfügbar.

3.3.2 Lokale Netze

Lokale Netze sind vergleichsweise einfach und insofern robust. Ausfälle sind selten, dann jedoch regelhaft nur durch Spezialisten analysierbar und zu beheben. Gleiches gilt für gängige Zugangstechniken zum Internet (Modem, ISDN-Karte, ISDN-Router etc.).

Aktive Angriffe auf lokale Netze, die deren Verfügbarkeit beeinträchtigen, sind eher theoretischer Natur. Dies nicht zuletzt deswegen, weil die angeschlossenen aktiven Komponenten (PC, Drucker etc.) "lohnendere" Angriffsziele darstellen.

3.3.3 Internet

Das Internet ist darauf ausgelegt, auch bei Ausfall einzelner Komponenten zu funktionieren. Verbindungen werden nach den aktuell verfügbaren Wegen ausgewählt; Daten, die aufgrund von Fehlfunktionen verlorengehen, werden erneut übermittelt. Dennoch gibt es keine Verfügbarkeitsgarantien, und bei Ausfall oder Störung bestimmter einzelner oder mehrerer zentraler Komponenten kann die Möglichkeit der Datenübermittlung auch für einen längeren Zeitraum (Stunden) gestört sein.

Zudem können Störungen bei den jeweiligen Service-Providern oder auf dem Weg dorthin auftreten. Da die Verbindung zum Service-Provider Punkt-zu-Punkt-förmig ist, bedeutet dies zunächst einen Totalausfall. Allerdings kann dies durch Ausweichen auf einen anderen Provider vergleichsweise einfach kompensiert werden.

Aktive Verfügbarkeitsstörungen des Internet sind kaum vorstellbar. Gerade aufgrund der geschilderten Robustheit und Fehlertoleranz wird es schwerlich gelingen, über längere Zeit spürbare Beeinträchtigungen zu erreichen.

3.3.4 Server

Als zentrale Komponente des Verfahrens steht die Verfügbarkeit des Servers und seiner Teilkomponenten im Vordergrund der Betrachtungen. Störungen an dieser Stelle wirken sich nicht nur auf einen Kunden, sondern auf alle Benutzer aus. Die Verfügbarkeit kann durch eine Vielzahl von Einflüssen äußerer Art (Stromausfall, Feuer), interner Art (Fehlbedienung, Überlastung) oder durch Angriffe aus dem Internet (Denial-of-Service-Angriffe) in Mitleidenschaft gezogen werden. Solche Einflüsse können jedoch zum einen durch geeignete Maßnahmen weitgehend ausgeschlossen werden und zum anderen ist es vergleichsweise einfach möglich, bei dennoch auftretenden Problemen das Verfahren und die Daten innerhalb kurzer Zeit auf einen anderen Server zu verlagern.

3.4 Authentizität

Daten, die von Dritten untergeschoben werden, tragen ein besonderes Risikopotenzial. In dem Maße wie der Empfängern dem vermeintlichen Absender Vertrauen entgegenbringt wird er auf eine Überprüfung verzichten, soweit diese überhaupt möglich ist. Ein Dritter kann daher u.U. lange Zeit unbemerkt Eingriffe in ein Verfahren vornehmen.

3.4.1 Client

Authentizitätsverletzungen im Client können erfolgen, wenn es einem Angreifer gelungen ist, den Client weitgehend unter seine Kontrolle zu bringen. Dies ist wie in 3.1.1 beschrieben möglich.

3.4.2 Lokale Netze

Während sich lokale Netze (wie beschrieben, s. 3.2.2) schlecht zur Datenveränderung eignen, ist ein Hinzufügen eher möglich. Dies setzt jedoch ein Umgehen der für den reibungslosen Betrieb solcher Netze implementierten Mechanismen voraus, die verhindern sollen, dass sich verschiedene Netzteilnehmer auf diese Weise ungewollt stören. Unter Berücksichtigung der Tatsache, dass ein solcher Eingriff nur bei Zugang zum lokalen Netz möglich ist, ist das konkrete Risiko im Zusammenhang mit Ki-ON als gering einzuschätzen.

3.4.3 Internet

Das Internet eignet sich aufgrund seiner Struktur besonders für sog. *Man-in-the-middle*-Attacken. Dabei trennt ein Angreifer eine bestehende Internetverbindung auf und begibt sich mit einem eigenen Rechner zwischen Sender und

Empfänger. Sämtliche Daten fließen dabei durch seine Station, können analysiert und manipuliert werden. Den jeweiligen Endgeräten kann dabei vorgespiegelt werden, dass sie weiterhin direkt kommunizieren. Vom Angreifer neu erzeugte, unterdrückte oder veränderte Daten werden daher als authentisch betrachtet. Da sich das Internet nicht kontrollieren lässt, müssen Maßnahmen in den Endgeräten selbst getroffen werden, um solche Attacken zu verhindern oder wenigstens feststellbar zu machen.

Zudem kann eine Station im Internet sich direkt als Ki-ON-Client oder als Ki-ON-Server ausgeben um auf diese Weise nichtauthentische Daten zu liefern. Auch dieser, weniger elaborierte Angriff ist entsprechend auszuschließen.

3.4.4 Server

Die Authentizität des Servers bzw. der dort erzeugten und gespeicherten Daten kann gefährdet werden, wenn das System durch einen Angreifer manipuliert bzw. kontrolliert wird (siehe 3.1.4). Da administrative Kräfte im Rahmen ihrer Tätigkeit eine weitgehende Kontrolle über den Server besitzen, ist ein solcher Missbrauch auch durch diese möglich.

4 Sicherheitsziele

Auf Grundlage der in Abschnitt 3 dargestellten Risiken werden hier Sicherheitsziele formuliert. Diese sind als Anforderung an das Gesamtsystem zu verstehen und durch geeignete Sicherheitsmechanismen zu gewährleisten. Die im Verfahren vorgesehenen und in der Praxis getroffenen Mechanismen werden in Folge an den genannten Zielen gemessen.

4.1 Need-to-know-Prinzip

Das Verfahren ist so auszugestalten, dass jeder Beteiligte (und Unbeteiligte) nur diejenigen Daten zur Kenntnis nehmen kann, die er für seine Tätigkeit benötigt. Dies bedeutet für die verschiedenen Rollen:

- Benutzer: dürfen nur auf die Daten zugreifen, die ihrer Einrichtung oder ihrem Sachgebiet entsprechend erforderlich sind; insbesondere der Zugriff auf Daten anderer Kunden ist zu verhindern.
- Zentrale Administratoren: dürfen Einzeldaten in der Regel nicht zur Kenntnis nehmen, haben gleichwohl aus technischen Gründen einen weitgehenden Datenzugriff. Dieser Widerspruch ist durch geeignete Maßnahmen soweit möglich aufzulösen.
- Externe: haben keinen berechtigten Zugriff auf die Daten; ihnen ist die Kenntnisnahme daher zu versperren.

Dabei ist zu beachten, dass es sich um Rollen, nicht um Personen handelt. Der Mitarbeiter einer Kindertageseinrichtung ist in diesem Sinne während der Arbeitszeit ein Benutzer, am Wochenende jedoch als Externer zu betrachten.

4.2 Geschlossene Benutzergruppe

Das Verfahren Ki-ON wird zwar über das offene Internet betrieben, ist jedoch an bestimmte vertragliche und technische Zugangsvoraussetzungen gebunden. Eine Benutzung darf nur dann möglich sein, wenn diese Voraussetzungen erfüllt werden. Dies bezieht sich sowohl auf Personen als auch auf Geräte, d.h. nur wenn ein zugelassener Benutzer ein zugelassenes Gerät verwendet, darf eine erfolgreiche Benutzung möglich sein. Aufgabe des Verfahrens ist es, zugelassene von nicht zugelassenen Benutzern und Geräten sicher zu unterscheiden.

4.3 Beweise statt Vertrauen

Das Verfahren Ki-ON wird über eine besonders offene und nicht vertrauenswürdige Infrastruktur abgewickelt. Im Gegensatz zu lokalen Client-Server-Verfahren, die auf bekannten, selbst kontrollierten Systemen betrieben werden, kann daher auf die Korrektheit von Behauptungen (etwa der Identität eines Servers, des Inhalts eines Datensatzes) nicht vertraut werden. Stattdessen sind solche Aussagen auf geeignete Weise zu beweisen. Dies sollte für den Endbenutzer in der Regel transparent erfolgen; in Zweifelsfällen sollte jedoch die Möglichkeit bestehen, dies benutzerseitig nachzuvollziehen.

4.4 Robustheit

Die Ki-ON-Kunden sind in höchstem Maße davon abhängig, dass das Verfahren wie vorgesehen funktioniert. Da sie über keine lokale Datenspeicherung verfügen, lassen sich Ausfallzeiten nicht überbrücken. Daher muss das Verfahren bis zur Schnittstelle beim Kunden äußerst robust ausgelegt sein; dies schließt die Verfügbarkeit von technischen Alternativen einzelner Systemteile ein.

5 Sicherheitsmechanismen

In diesem Abschnitt werden die Sicherheitsmechanismen, die im Verfahren Ki-ON getroffen wurden, beschrieben und aus konzeptioneller Sicht bewertet. Eine Bewertung in der Praxis erfolgt in Abschnitt 6.

5.1 Server

5.1.1 Darstellung

Für den Ki-ON-Server wird das Betriebssystem Linux (Kernel 2.4.5) verwendet. Dabei handelt es sich um eine Quellcode-offene Variante des kommerziellen Betriebssystems UNIX. Als Web-Server kommt das Open-Source-Produkt Apache zum Einsatz. Auf dem Ki-ON-Server werden nur ausgewählte Dienste betrieben; dies sind:

- HTTPS – zur Bereitstellung des Ki-ON-Service über das Internet
- SSH – zur Administration der Ki-ON-Server über das Internet
- ftp – für Dateitransfers über das Internet
- DNS – zur Auflösung von Domainnamen und IP-Adressen im Internet

- ntp – zur Zeit-Synchronisation über das Internet
- MySQL – zum internen Betrieb des Datenbanksystems

Durch entsprechende Einstellungen in den Diensten bzw. in der Firewall (siehe 5.2) wird sichergestellt, dass aus dem Internet auf direkte Weise nur HTTPS und SSH erreichbar sind. Bei HTTPS handelt es sich um einen Dienst, der eine über SSL (siehe 5.3) gesicherte HTTP-Verbindung zur Verfügung stellt; diese wird im Zuge der normalen Verwendung des Ki-ON-Systems durch die Kunden verwendet. SSH (Secure Shell, siehe 5.4) ermöglicht einen gesicherten Zugriff auf Systemebene zum Zwecke der Administration oder für Datentransfers. Dieser Dienst wird nicht von den Kunden, sondern ausschließlich vom Betreiber des Ki-ON-Systems genutzt. Zum Schutz vor Pufferüberläufen wird auf dem Server das Produkt libsafe verwendet.

5.1.2 Bewertung

Das verwendete Betriebssystem Linux ist seit Jahren als bewährte Server-Plattform bekannt und ist insbesondere für den Betrieb von Web-Servern weltweit im Einsatz. Apache stellt einen der führenden Web-Server dar und ermöglicht eine weitgehend problemlose Integration von SSL. Durch die weite Verbreitung dieser Software erfolgt eine ständige Weiterentwicklung in Form von Updates und Patches. Unter Berücksichtigung dieser Pflegemaßnahmen ist es ohne weiteres möglich, ein sicheres System nach dem Stand der Technik zu betreiben. Zu den gleichwohl vorhandenen konzeptionellen Schwächen und Stärken von UNIX und daraus abgeleiteten Betriebssystemen siehe z.B. [Kühn/Schläger 1997].

Hinsichtlich der Verfügbarkeit ist im Zusammenhang mit dem Internet vor allem die Robustheit gegen Denial-of-Service-Angriffe zu bewerten. Das Betriebssystem Linux verfügt im Netzwerk-Kern über eine Sicherung gegen einfache DoS-Angriffe, die darauf beruhen, ungewöhnliche Netzwerkpakete zu versenden, die aufgrund mangelhaft programmierter Netzwerksoftware zum Absturz des Rechners oder zum Stillstand des Netzwerks führen. Zudem existieren Vorkehrungen gegen den Versuch, eine Vielzahl halboffener TCP-Verbindungen herzustellen, bis alle dafür verfügbaren Systemressourcen aufgebraucht sind und damit kein regulärer Kontakt mehr möglich ist (sog. SYN-Flood-Attacke). Gegen aufwändigere Formen des DoS wie etwa verteilte DoS-Angriffe, bei denen ein Server gleichzeitig von einer Vielzahl von "ferngelenkten" Rechnern mit normalen Anfragen traktiert wird, so dass kein anderer Benutzer mehr zugreifen kann, hilft diese Maßnahme jedoch nicht. Einem solchen Angriff stehen alle heutigen Server vergleichsweise machtlos gegenüber; allenfalls eine entsprechend großzügig ausgelegte Systemleistung kann vorbeugend dagegen unternommen werden. Zu weiteren Empfehlungen, die jedoch weniger Serverbetreiber, sondern vor allem Netzvermittler betreffen, siehe [BSI 2000].

Libsafe ermöglicht einen Schutz vor bestimmten Puffer-Überläufen, die mit Hilfe einiger Systemfunktionen (in der aktuellen Version 2.0 strcpy, strcat, getwd, gets, [vf]scanf, realpath, [v]sprintf) erzeugt werden können. Dies wird durch Ersetzen der entsprechenden Systembibliotheken durch sichere Versionen erreicht. Damit können eine Reihe von Problemen vermieden werden, das allgemeine Problem des Puffer-Überlaufs wird dadurch allerdings nicht gelöst. Es ist insofern weiterhin mit Programmen zu rechnen, die in dieser Hinsicht die Systemsicherheit gefährden. Dem kann proaktiv allerdings kaum vorgebeugt werden.

Sicherheitswarnungen und Patches der eingesetzten Programme sollten jedoch beachtet bzw. zügig eingespielt werden.

5.2 Firewall

5.2.1 Darstellung

Der Ki-ON-Server verwendet den integrierten Paketfilter, der durch das Betriebssystem Linux bereitgestellt wird. Dieser Filter ermöglicht eine Kontrolle der Datenströme in, durch und aus der Netzwerkschnittstelle auf Basis einzelner IP-Pakete. Dabei kann neben der IP-Adresse und dem TCP- bzw. UDP-Port eine Vielzahl weiterer Parameter für die Entscheidung, wie mit einem Paket verfahren werden soll, herangezogen werden. Dies betrifft insbesondere TCP-Flags zur Verbindungssteuerung, da diese häufig missbräuchlich verwendet werden, um Server zu attackieren und lahm zu legen.

Eine Kontrolle auf Inhalts- bzw. Dienstebene ist mit diesem Paketfilter nicht möglich. So kann zwar ein bestimmter TCP-Port (z.B. Port 80), auf dem standardmäßig ein bestimmter Dienst läuft (http bzw. WWW), kontrolliert werden; eine Kontrolle darüber, dass auf diesem Port nicht ein anderer Dienst bzw. dieser Dienst nicht missbräuchlich genutzt wird, ist jedoch nicht möglich.

Der Ki-ON-Paketfilter ist so eingestellt, dass nur die zur Erbringung der angebotenen Dienstleistungen erforderlichen Pakete akzeptiert werden; alle anderen Pakete werden mit einer Fehlermeldung an den Absender zurückgewiesen und auf dem Server protokolliert; eine Auswertung der Protokolle erfolgt durch ein entsprechendes Werkzeug (psad; port scan attack detector). Dieses Verhalten ist sowohl für eingehende als auch für ausgehende Pakete eingestellt. Eine Weiterleitung von Paketen erfolgt nicht.

5.2.2 Bewertung

Die Verwendung des Linux-Paketfilters stellt eine Basissicherung gegen missbräuchliche Zugriffe bzw. fehlerhafte oder bösartige Pakete aus dem Internet dar, die den Serverbetrieb beeinträchtigen oder als Hilfsmittel dienen können, um Sicherheitsvorkehrungen zu unterlaufen. Bei einer – wie bei Ki-ON geschehen – restriktiven Konfiguration des Filters wird eine Reihe von Beeinträchtigungen dieser Art verhindert. Das verwendete Auswertungs- und Alarmierungstool ermöglicht zudem eine Reaktion auf Angriffe in Echtzeit, sofern die damit zur Verfügung gestellten Möglichkeiten genutzt werden.

Gleichwohl ist das Konzept, Firewall und Server auf einer Maschine gemeinsam unterzubringen, mit prinzipiellen Schwächen behaftet. Werden auf einem Gerät, das ausschließlich Sicherheitszwecken dient – und ein solches stellt eine Firewall dar – auch andere Dienste betrieben, besteht die Gefahr, dass durch Angriff auf diese Bereiche auch Einfluss auf die Sicherheitsfunktionalität genommen werden kann. Eine Firewall sollte daher stets dediziert betrieben werden, um schädliche Wechselwirkungen mit anderer dort aktivierter Software auszuschließen.

Es ist daher zu empfehlen, eine eigenständige Firewall einzurichten, die ausschließlich für diesen Zweck verwendet wird und keine nach außen gerichteten Serverdienste bereitstellt. Dabei sollte erwogen werden, ein anderes Betriebssystem als auf den Ki-ON-Servern zu verwenden. Dies bietet insofern einen

Sicherheitsvorteil als ein Angreifer dann mit verschiedenen Systemen zu tun hat, die angegriffen werden müssen und einzelne Sicherheitslücken nicht durchgängig ausgenutzt werden können.

5.3 Secure Sockets Layer (SSL)

5.3.1 Darstellung

Für die Absicherung der Kommunikation zwischen Client und Server wird SSL v3 [Freier1996] verwendet. Dieses Protokoll ist ein offener Standard und wird daher von den marktüblichen Web-Browsern und anderer Client-Software beherrscht. Es handelt es sich um ein anwendungsunabhängiges Protokoll zur Erzielung von Transaktionssicherheit im Internet. Mit Hilfe von SSL können folgende Ziele erreicht werden:

- Authentizität durch gesicherten Nachweis der Identität der Endpunkte auf Grundlage von Zertifikaten
- Vertraulichkeit durch Verschlüsselung des Datenaustausches zwischen den Endpunkten einer Verbindung
- Integrität durch Signierung des Datenaustausches zwischen den Endpunkten einer Verbindung

Im Verfahren Ki-ON steht dafür serverseitig eine Triple-DES-Verschlüsselung mit 168 bzw. 112 Bit Schlüssellänge zur Verfügung; die Signierung erfolgt mit SHA-1 und 160 Bit. Zur Serverauthentisierung dient ein Zertifikat, das von einer anerkannten Zertifizierungsstelle ausgestellt wurde. Eine ebenfalls durch SSL mögliche Authentisierung des Clients erfolgt bei Ki-ON nicht.

5.3.2 Bewertung

SSL wurde von der Firma Netscape entwickelt und stellt den zurzeit wichtigsten Standard zur Sicherung von internetbasierten Verbindungen in offenen Benutzergruppen dar. Das Protokoll vereint die dafür wichtigen Bedingungen der Flexibilität und der Transparenz für den Benutzer mit einer bewährten Sicherheit. Da SSL für das offene Internet entwickelt wurde, müssen beide Kommunikationspartner flexibel auf die jeweiligen technischen Fähigkeiten und Anforderungen des Gegenübers reagieren können. Client und Server handeln dabei im Rahmen des Verbindungsaufbaus aus, ob und in welcher Form SSL zum Einsatz kommt. Daher sind Art und Qualität der verwendeten Mechanismen (z.B. Verschlüsselungsalgorithmen und Schlüssellängen) nicht starr vorgegeben, sondern aus einer Vielzahl von definierten Varianten auswählbar. In der Regel verständigen sich Client und Server auf das jeweils beste gemeinsam verfügbare Verfahren, jedoch können durch Konfiguration vor allem auf Server-Seite auch andere Verhaltensweisen (z.B. Mindeststandards) festgelegt werden.

In jedem Fall beinhaltet eine SSL-Verbindung eine Authentisierung des Servers gegenüber dem Client sowie eine Integritätssicherung der übertragenen Daten. Diese Elemente sind nicht verzichtbar, d.h. Fehler in diesem Bereich führen zu einem Verbindungsabbruch. Die Verschlüsselung selbst sowie die Authentisierung des Clients gegenüber dem Server sind optional; üblicherweise wird eine Verschlüsselung mit Schlüsselstärken zwischen 40 und 128 Bit verwendet sowie auf eine Clientauthentisierung verzichtet.

Die aktuelle Version von SSL ist 3.0; diese auch bei Ki-ON verwendete Version verfügt gegenüber der Vorgängerversion 2.0 über eine Reihe sicherheitsrelevanter Verbesserungen. Dennoch wird SSL 2.0 noch vielfach eingesetzt und aus Kompatibilitätsgründen auch von modernen Browsern akzeptiert. Der offizielle Standard TLS (Transport Layer Security), der auf SSL basiert, hat sich bislang nicht durchgesetzt.

5.3.2.1 Authentisierung

Die Authentisierung der Endpunkte einer SSL-Verbindung ist für beide Kommunikationspartner möglich; üblich ist jedoch nur die Serverauthentisierung. Der Identitätsnachweis basiert auf Grundlage von Zertifikaten, d.h. elektronisch signierter digitaler Ausweise, die von besonderen Stellen (sog. Certificate Authorities, CA) ausgestellt werden. Diese stellen sicher, dass die Identitätsangaben in den Ausweisen korrekt sind; ihnen muss daher vertraut werden. In technischer Hinsicht muss zur Überprüfung eines vorgelegten Zertifikats ein Wurzel-Zertifikat der entsprechenden CA vorliegen. Für gängige Anbieter sind diese in den Standardbrowsern bereits fest implementiert. Im Verfahren Ki-ON wird ein Zertifikat einer in diesem Sinne wohlbekannten Zertifizierungsstelle verwendet; das Zusammenspiel mit gängigen Browsern ist daher unproblematisch.

Während bei SSL eine Server-Authentisierung zwingend ist, ist die Client-Authentisierung optional. Dies liegt im Wesentlichen darin begründet, dass der erforderliche Aufwand, ein entsprechendes Zertifikat zu erhalten, für den Endbenutzer vergleichsweise hoch ist und zudem auf Server-Seite andere Möglichkeiten der Authentisierung (in der Regel mit Kennung und Passwort) existieren, die mit geringerem Aufwand verbunden sind. Auch bei Ki-ON wird auf eine SSL-basierte Clientauthentisierung verzichtet. Allerdings handelt es sich um eine geschlossene Benutzergruppe, für die die Einrichtung entsprechender Zertifikate im Rahmen der vertraglichen Beziehungen durchaus möglich wäre (s.a. 5.6.2).

5.3.2.2 Verschlüsselung

Der Ki-ON-Server bietet mit Triple-DES die bestmögliche Verschlüsselungsstärke des SSL-Protokolls an. Triple-DES basiert auf dem Verfahren Digital Encryption Standard, das mit 56-Bit-Schlüsseln arbeitet, und erhöht dessen kryptografische Stärke durch Mehrfachverschlüsselung mit zwei (112 Bit effektive Schlüssellänge) oder drei (168 Bit effektive Schlüssellänge) verschiedenen Schlüsseln. Beide Varianten verfügen damit über einen Level, der heute als nicht brechbar gilt. Das heißt, die Vertraulichkeit entsprechend gesicherter SSL-Verbindungen kann durch bekannte kryptanalytische Verfahren nicht verletzt werden.

Da nicht alle Browser mit einer solchen starken Verschlüsselung umgehen können, bietet der Ki-ON-Server auch schwächere Algorithmen bzw. Schlüssellängen an. Diese sind teilweise darauf ausgelegt, Dritten (nämlich US-amerikanischen Geheimdiensten) die Entschlüsselung zu ermöglichen und können daher nicht als sicher gelten. Im Verfahren Ki-ON sollte daher davon kein Gebrauch gemacht werden.

5.3.2.3 Signierung

In Kombination mit Triple-DES bietet der Ki-ON-Server die Integritätssicherung durch das kryptografische Prüfsummenverfahren SHA-1 mit 160 Bit Schlüssel-

länge an. Der Secure Hash Algorithm ist ein bewährter Standard und vom Algorithmus und der verwendeten Schlüssellänge gegen bekannte Angriffe ausreichend sicher.

Auch der andere von SSL angebotene Algorithmus, MD5 (Message Digest 5) mit 128 Bit Schlüssellänge ist als sicher und ausreichend gegen Attacken bekannt.

5.4 Secure Shell (SSH)

SSH wird bei Ki-ON ausschließlich für administrative Zwecke verwendet; Kunden verwenden dieses Protokoll nicht.

5.4.1 Darstellung

Bei SSH handelt es sich um ein (in der Version 2.x) standardisiertes Protokoll für den sicheren Fernzugriff über unsichere Netze. Ähnlich wie bei SSL erfolgt die Sicherung durch kryptografische Mechanismen, wobei sich die Protokolle im Detail jedoch erheblich voneinander unterscheiden. Hauptanwendungsgebiet für SSH stellt das Anmelden an entfernten Maschinen dar (ssh bzw. slogin), aber auch andere Anwendungen (z.B. scp, secure copy) sind verfügbar. Der gesamte Datenstrom zwischen Client und Server wird dabei gegen eine missbräuchlichen Kenntnisnahme und eine willkürliche Veränderung durch Dritte geschützt.

Neben kommerziellen Implementationen des Protokolls ist mit OpenSSH eine frei verfügbare Version erhältlich, die ab Version 2.1.0 auch SSH 2.x beherrscht. Diese Software ist für verschiedene Betriebssysteme, vor allem UNIX-basierten, verfügbar. Die verschiedenen SSH-Implementationen verwenden aus urheberrechtlichen und sicherheitstechnischen Erwägungen teilweise unterschiedliche Kryptgorithmen; der aktuell verwendete Algorithmus wird jeweils zwischen Client und Server ausgehandelt.

5.4.2 Bewertung

SSH hat sich seit geraumer Zeit als kryptografisch sicher und gegen bekannte Angriffsformen als robust erwiesen. Allerdings hat die Version 1 des Protokolls bekannte Schwächen und sollte daher nicht mehr verwendet werden. In Version 2 wurden diese Schwächen beseitigt. Für einzelne Implementationen (sowohl kommerziell als auch frei) sind besondere Sicherheitsprobleme bekannt, die sich teilweise jedoch nur auf bestimmte Betriebssysteme beziehen. Hier gilt, wie überall, dass jeweils die aktuelle Version des Produkts verwendet werden sollte und eventuell verfügbare Patches eingespielt werden sollten. Unter diesen Voraussetzungen können die mit SSH bezweckten Schutzziele problemlos erfüllt werden.

5.5 Benutzerauthentisierung

5.5.1 Darstellung

Jeder Ki-ON-Benutzer verfügt im System über eine eigene, persönliche Kennung, die mittels eines Kennworts geschützt ist. Vor der Benutzung des Systems bzw. dem Zugriff auf Daten müssen Kennung und zugehöriges Kennwort eingegeben werden. An die Zusammensetzung der Kennwörter werden vom System keine besonderen Anforderungen gestellt. Eine direkte Änderung des Kennworts durch den Benutzer ist nicht möglich.

Die Anmeldung bzw. der Versuch einer Anmeldung ist mit einer konstanten Verzögerung verbunden, bevor entweder ein Zugriff auf das Verfahren erfolgt oder – im nicht erfolgreichen Fall – wieder die Anmeldemaske erscheint. Die Frequenz möglicher Anmeldeversuche wird dadurch begrenzt. Nach erfolgter Anmeldung wird die Benutzeridentifizierung über eine Sitzungskennung hergestellt, der mittels eines Cookies oder als Teil der URL (sog. URL rewriting) an den Server übermittelt wird. Dabei handelt es sich um eine gängige Methode zur Sitzungssteuerung im ansonsten zustandslosen Protokoll HTTP.

5.5.2 Bewertung

Eine funktionierende, mißbrauchsresistente Benutzerauthentisierung stellt die Grundlage einer Reihe daran anknüpfender Sicherheitsmaßnahmen wie Zugriffskontrolle, Protokollierung etc. dar. Daher sind an die Mechanismen für eine korrekte Identifizierung der Benutzer insgesamt hohe Anforderungen zu stellen.

Die im Ki-ON-System vorgesehenen Maßnahmen können diese Anforderungen jedoch nur zum Teil erfüllen. Zwar werden die Authentisierungsdaten erst nach Herstellung der geschützten Verbindung mittels SSL übertragen und sind insofern gegen eine unbefugte Kenntnisnahme auf der Transportstrecke geschützt. Allerdings können Kennwörter auch auf andere Weise zur Kenntnis genommen werden (z.B. wenn sie notiert werden oder durch anwesende Dritte während ihrer Eingabe). In solchen Fällen, in entsprechenden Verdachtsfällen oder auch nur als vorbeugende Maßnahme müssen Kennwörter zum einen durch den Benutzer jederzeit änderbar sein und zum anderen durch das System einer gewissen Verfallszeit unterworfen werden. Nur wenn zudem der Benutzer die Möglichkeit hat, das Kennwort selbst zu bestimmen (im Rahmen vorgegebener Anforderungen wie Mindestlänge und Komplexität), kann vermieden werden, dass Kennwörter so schwer zu merken sind, dass sie notiert werden und damit das Missbrauchsrisiko unnötig erhöht wird.

Insgesamt wird daher eine Kennwortverwaltung empfohlen, die sich (auf Grundlage des BSI-Grundschutzkonzepts [BSI]) an folgenden Richtwerten orientiert:

- Das Kennwort sollte mindestens 6 Zeichen lang sein.
- Das Kennwort sollte nicht nur aus Buchstaben bestehen (mindestens ein Sonderzeichen oder eine Ziffer).
- Das Kennwort muß regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Die Wahl von Trivialkennwörtern ("123456", "qwertz") sollte verhindert werden.
- Nach mehrfacher (max. fünffacher) fehlerhafter Eingabe des Kennworts sollte eine Sperrung der Kennung erfolgen.

Diese Bedingungen sollten nicht nur als Anforderung an die Benutzer formuliert werden, sondern vom Ki-ON-System technisch erzwungen werden.

Die Identifizierung durch Sitzungs-ID vermeidet eine wiederholte Eingabe des Kennworts. Da Sitzungen bei Kenntnis der ID von Dritten übernommen werden können, handelt es sich bei diesen Werten um äußerst schützenswerte Daten. Gegen eine unberechtigte Kenntnisnahme sind sie durch die SSL-Verschlüsselung geschützt. Ein Erraten ist aufgrund des komplexen Aufbaus der

Sitzungs-ID äußerst schwierig und kommt als realistisches Angriffsszenario daher nicht in Betracht.

Eine konstante Login-Verzögerung setzt ein gewisses Limit für die Möglichkeit, eine gültige Benutzeranmeldung durch Probieren zu erlangen. Um eine unnötige Verzögerung für berechnigte Benutzer, die sich ausnahmsweise fehlerhaft anmelden, zu vermeiden, kann diese Begrenzung jedoch nicht allzu eng ausfallen. Besser wäre daher eine dynamische Verzögerung, die umso länger wird, je öfter ein Fehlversuch (mit gleicher Kennung, mit gleicher Session-ID oder gleicher IP-Adresse) in Folge stattfindet.

5.6 Terminalauthentisierung

5.6.1 Darstellung

Jedes Ki-ON-Endgerät wird mit Hilfe eines Terminal-Kennworts identifiziert. Dieses muss bei erstmaliger Benutzung eingegeben werden und steht danach an dem Gerät zur wiederholten Identifikation gegenüber dem Server zur Verfügung. Eine neue Eingabe muss nur in Problemfällen oder nach längerer Nichtbenutzung erfolgen. Mit diesem Verfahren wird die Verwendung eines fremden Computers zur Bearbeitung der Daten erschwert. Mitarbeitern ist es auf diese Weise zum Beispiel nicht ohne weiteres möglich von ihrem privaten Computer aus auf die Daten der Einrichtung zuzugreifen.

Die Terminalauthentisierung wird technisch mittels eines Cookies umgesetzt. Ist ein geeignetes Cookie zur Identifikation des Geräts vorhanden, und wird dies vom Browser zum Ki-ON-Server übermittelt, gilt das Endgerät als authentisch. Andernfalls wird der Benutzer aufgefordert, das Terminalkennwort einzugeben; ist dies korrekt, wird ein Cookie an den PC übermittelt, das dann bei den folgenden Anmeldungen verwendet wird. Dieses Cookie enthält einen zehnstelligen alphanumerischen Code, der nicht mit dem Terminalkennwort identisch ist.

5.6.2 Bewertung

Für einen externen Angreifer stellt die Terminalauthentisierung zunächst eine zusätzliche Hürde dar, um von einem Fremdgerät aus auf das Verfahren zuzugreifen. Neben der Kennung eines Benutzers ist auch das zugehörige Terminalkennwort oder das entsprechende Cookie erforderlich. Für den Fall, dass es gelingt, eine Ki-ON-Anmeldung im Netz zu belauschen (wogegen jedoch die SSL-Verschlüsselung schützt), stehen allerdings sämtliche erforderlichen Daten zur Verfügung. Nur für den (unwahrscheinlichen) Fall, dass zwar eine Benutzerkennung bekannt ist, das zugehörige Terminalkennwort aber nicht, ist ein Sicherheitsgewinn feststellbar.

Für einen Internen stellt die Terminalauthentisierung in der implementierten Form kein wesentliches Hindernis gegen einen Zugriff von einem anderen Gerät (z.B. von Zuhause) dar, da es genügt, das Cookie dort einzutragen. Die Möglichkeit, auf das Cookie zuzugreifen, um es zu exportieren, kann aus prinzipiellen Gründen nicht verhindert werden. Auch ohne Kenntnis des Terminalkennworts kann er daher das Verfahren mit seiner Benutzerkennung von beliebigen Geräten aus nutzen.

Insgesamt ist festzustellen, dass die gewählte Form der Terminalauthentisierung mit Hilfe von Cookies bedeutet, dass Authentisierungsdaten vergleichsweise ungeschützt im PC gespeichert vorliegen. Je nach verwendetem Browser und Betriebssystem kann jeder Benutzer oder jeder Benutzer mit ausreichenden Rechten diese Daten einsehen, kopieren und auch ändern. Ein Missbrauch ist daher schwer zu verhindern. Zudem ist es erforderlich, die Verwendung von Cookies im Browser zuzulassen, was ggf. mit den aus Sicherheits- und Datenschutzgründen getroffenen Restriktionen beim Anwender kollidiert. Während andere bei Ki-ON verwendete Cookies (zum Session-Management) nicht zwingend erforderlich sind, führt die Ablehnung des Cookies zur Terminalidentifizierung dazu, dass das Terminalkennwort bei jeder Anmeldung eingegeben werden muss; ein wenig sinnvoller Zustand.

Aus den genannten Gründen stellt die Verwendung von Cookies zur Terminalidentifizierung keine optimale Lösung dar. Da im Rahmen von Ki-ON auf die von SSL zur Verfügung gestellten Funktionalitäten zurückgegriffen werden kann, bietet es sich an, die dabei optionale Client-Authentisierung zu nutzen. Die zugelassenen Endgeräte müssen dazu mit einem Client-Zertifikat ausgestattet werden, das bei der Errichtung der SSL-Verbindung an den Server übermittelt wird. Dieser kann dann anhand des vorgelegten Zertifikats überprüfen, ob sich das Endgerät im Kreis der zugelassenen Clients befindet und unbekannte Geräte bereits in dieser Phase abweisen. Dies erschwert einem Angreifer das Eindringen in das System zusätzlich, da er dann nicht einmal bis zur Eingabemaske für Kennung und Kennwort vorgelassen wird. Die Client-Zertifikate sollten, um Kosten und Aufwand auf Kundenseite zu vermeiden, durch den Betreiber erzeugt und vergeben werden und dem Kunden auf sicherem Weg zugestellt werden.

Im Gegensatz zu Cookies unterliegen Zertifikate in der Regel einem besseren Schutz im lokalen System, so dass ein Export oder eine andere missbräuchliche Verwendung leichter zu verhindern ist.

5.7 Zugriffsschutz

5.7.1 Darstellung

Das Ki-ON-System bzw. die zu Grunde liegende Datenbank implementieren Mechanismen, die dafür sorgen, dass jeder angemeldete Benutzer nur auf diejenigen Daten zugreifen kann, die ihm berechtigt zur Verfügung stehen. Mitarbeiter der Trägerorganisationen erhalten nur Zugriff auf Daten, die sie nach den Bestimmungen des Datenschutzes erhalten dürfen. Sie erhalten insbesondere keinen Zugriff auf personenbezogene Daten, sondern können nur anonymisierte Statistiken abrufen.

Bei Ki-ON wird das relationale Datenbanksystem MySQL verwendet, eine Open-Source-Lösung, die vor allem im Zusammenhang mit Internet-basierten Angeboten verwendet wird, da sie sich über entsprechende Programmiersprachen wie Perl oder PHP besonders gut steuern lässt. MySQL bietet die vom Standard SQL (Structured Query Language) her bekannten sowie eine Reihe von erweiterten Zugriffsschutzmechanismen, um sicherzustellen, dass nur berechtigte Benutzer auf Daten zugreifen können und diese nur im Rahmen des Zugelassenen. Die Berechtigungen werden dabei selbst in speziellen Datenbanktabellen gespeichert und vom Datenbankadministrator verwaltet.

5.7.2 Bewertung

Das verwendete Datenbanksystem bietet nur begrenzte Möglichkeiten der Zugriffsteuerung. Insbesondere sind sogenannte Views nicht implementiert. Andere Datenbanksysteme verfügen in dieser Hinsicht über mehr Funktionalität. Allerdings handelt es sich hierbei in der Regel um vergleichsweise kostspielige Datenbanklösungen, die möglicherweise unter Aufwandserwägungen nicht in Frage kommen.

Da es bei Ki-ON erforderlich ist, die Zugriffsrechte weitaus differenzierter zu vergeben, als dies durch MySQL unterstützt wird, findet die Zugriffsverwaltung auf der Programmebene statt. Dies schränkt zum einen die Administrierbarkeit und die Transparenz des Systems ein. Zum anderen besteht die Gefahr, dass der Zugriffschutz ausgehebelt wird, sofern es Unbefugten gelingt, direkt auf das Datenbanksystem zuzugreifen.

Die von Ki-ON verwendete Sprache PHP ist sehr mächtig, und der Interpreter, der in den Webserver als Modul oder als separate CGI-Version eingebunden ist, kann auf Dateien zugreifen, Befehle ausführen und Netzwerkverbindungen zu einem Server herstellen. Diese Eigenschaften können den Webserver unsicher machen. Aus diesem Grund sind eine Reihe von Installations- und Konfigurationsaspekten zu berücksichtigen. Wird PHP als Web-Server-Modul betrieben, so erbt der Interpreter die Ausführungsrechte des Server-Prozesses. Dieser sollte daher als besonderer Benutzer laufen, und in keinem Fall als "root". Dieser spezielle Benutzer sollte nur die notwendigen Rechte im gesamten Dateisystem besitzen und daher auf Bereiche außerhalb der HTML-Dokumente und Skripte keinerlei Zugriff haben. Auf diese Weise kann gewährleistet werden, dass eventuelle Programmierfehler in den Skripten nicht über diese Bereiche hinausgehende Auswirkungen haben. Wird PHP als CGI-Version betrieben, d.h. vom Web-Server über das Common Gateway Interface aufgerufen, sollte der Interpreter nicht im cgi-bin-Verzeichnis selbst liegen, sondern an einer Stelle außerhalb des vom Web-Server erreichbaren Bereichs. Dies erfordert zwar die Einbindung einer Shell-Escape-Zeile (wie etwa "#!/usr/local/bin/php") in den Skripten, erhöht aber die Sicherheit erheblich. Für weitere Details siehe [Schmid 2000].

5.8 Tripwire

5.8.1 Darstellung

Auf dem Ki-ON-Server wird als zusätzliche Sicherheitsmaßnahme das Produkt "Tripwire" eingesetzt. Dabei handelt es sich um eine Software zur Kontrolle der System-Integrität, mit deren Hilfe Manipulationen oder andere unerwünschte Änderungen an Dateien – insbesondere an Programmen – bzw. Verzeichnissen entdeckt werden können. Tripwire existiert sowohl in kommerziellen Versionen für verschiedenen Plattformen als auch als Open-Source-Produkt für Linux (www.tripwire.org).

Tripwire basiert auf dem Abgleich des aktuellen Systemzustands gegen einen Sollzustand, der in einer Datenbank hinterlegt ist. Wird eine Differenz dieser beiden Werte festgestellt, bedeutet dies, dass eine Änderung des Systemzustands stattgefunden hat, und es wird ein entsprechender Alarm für den Systemadministrator ausgelöst. Aus Effizienz- und Speicherplatzgründen werden nicht die Dateien als solche, sondern geeignete Hash-Werte miteinander verglichen.

Dafür stehen verschiedene Verfahren zur Verfügung, die sich in ihrer Performanz und Sicherheit deutlich voneinander unterscheiden.

5.8.2 Bewertung

Neben der Auswahl der Hash-Algorithmen kann Tripwire hinsichtlich der Dateien bzw. Verzeichnisse konfiguriert werden, die kontrolliert werden sollen. Sinnvollerweise sind nur solche Dateien überwachbar, die keiner oder nur einer gelegentlichen Änderung unterworfen sind (Programme, Konfigurationsdateien, Bibliotheken etc.), da jede autorisierte Änderung einer solchen Datei eine entsprechende Änderung der Tripwire-Datenbank erforderlich macht. Insofern ist eine Abwägung zwischen Sicherheit und Administrationsaufwand erforderlich. In jedem Fall sollten alle Programme und zugehörige Konfigurations- und ggf. Datendateien überwacht werden, die mit besonderen Privilegien ausgestattet sind (d.h. mit Super-User-Rechten oder mit den Rechten eines anderen Benutzers, der Zugriff auf sicherheitsrelevante Systemteile hat). Das gleiche gilt für diejenigen Serverprogramme und zugehörige Elemente, die ihren Dienst ins Internet anbieten, da diese primär von entsprechenden Attacken betroffen sind.

Zusätzlich sollten folgende Maßnahmen ergriffen werden, um eine Tripwire-Installation gründlich abzusichern:

- Das Tripwire-System (d.h. die Datenbank und das Tripwire-Programm) sollte auf einem Datenträger gespeichert werden, der physikalisch gegen ein Überschreiben gesichert ist (z.B. eine schreibgeschützte Diskette oder eine CD-ROM). Nur so kann sichergestellt werden, dass nicht mit einer Änderung am System zugleich die Tripwire-Vergleichswerte geändert werden und damit der Schutz zunichte gemacht wird.
- Die Tripwire-Datenbank sollte nur dann erzeugt werden, wenn die Integrität des Systems gewährleistet ist. Dies ist in der Regel nur dann der Fall, wenn das System neu installiert worden ist.
- Es sollten kryptografisch sichere Hash-Algorithmen verwendet werden (MD5, Snefru, MD4, MD2, SHA oder Haval). Die ebenfalls verfügbaren CRC-Algorithmen garantieren keine Sicherheit gegen eine gezielte Manipulation. Möglichst sollten wenigstens zwei verschiedenen Verfahren zugleich zum Einsatz kommen; dies schließt die Ausnutzung möglicherweise vorhandener Schwächen eines einzelnen Verfahrens aus.
- Als zusätzliche Maßnahme sollte die Tripwire-Datenbank ausgedruckt oder auf einem anderen, physikalisch vom zu sichernden System getrennten Datenträger gespeichert werden. Dies erlaubt in Zweifelsfällen eine manuelle Kontrolle auf einzelne Veränderungen.

6 Überprüfung der Sicherheitsmechanismen

Um die getroffenen und oben beschriebenen Mechanismen in der Praxis zu überprüfen, wurde der Ki-ON-Server über das Internet einer Reihe von teilweise automatisierten, teilweise manuellen Tests unterworfen. Die Ergebnisse dieser Überprüfung sind im Folgenden aufgeführt.

6.1 Server

Als Ki-ON-Server steht *s1.ki-on.net* zur Verfügung; dieser ist von der Ki-ON-Homepage www.ki-on.de aus direkt erreichbar. Die IP-Adressauflösung (host, nslookup) lässt diesen Server als 213.83.36.18 erkennen (autorisierter Nameserver ns1.geumann.net).

6.1.1 Internetanbindung

Das Domainlisting für *ki-on.net* ergibt:

```
> ls ki-on.net
[ns1.geumann.net]
$ORIGIN ki-on.net.
@                1D IN A      213.61.10.181
*                1D IN A      213.61.10.181
ftp              1D IN A      213.61.10.181
www.ftp         1D IN A      213.61.10.181
mail            1D IN A      213.61.10.181
www.mail        1D IN A      213.61.10.181
s1              1D IN A      213.83.36.18
www.s1          1D IN A      213.83.36.18
www             1D IN A      213.61.10.181
```

Ergebnis der whois-Abfrage beim Registrar "Core" (www.corenic.net):

```
Jens Vonderheide (template COCO-750662)
jvonderheide@redlink.de
Ruedesheimerstr. 2a
Bremen, Bremen 28199 Deutschland

Domain Name: ki-on.net
Status: production

Admin Contact, Technical Contact:
Jens Vonderheide (COCO-750662) jvonderheide@redlink.de
+49 421 5977956 (FAX) +49 421 5977957
Zone Contact:
Stefan Geumann (COCO-226450) hostmaster@domainer.de
+49 700 366 246 37 (FAX) +49 231 6 10 80 23

CORE Registrar: [CORE-81]

Record created: 2000-11-26 13:17:26 UTC by [CORE-81]
Record expires: 2001-11-26 07:19:44 UTC

Domain servers in listed order:

ns1.geumann.net 62.116.129.62
ns2.geumann.net 213.185.128.229

Database last updated on 2001-07-14 16:25:43 UTC
```

Ein traceroute-Aufruf meldet:

```
> traceroute -O s1.ki-on.net
traceroute to s1.ki-on.net (213.83.36.18), 30 hops max, 40 byte packets
...
5  E-FRA-kle-Rlp810.defra.ecs-ip.net (212.38.221.18) hostmaster@energis-
ecs.com
6  Plusline-Network.defra.ecs-ip.net (212.38.219.14) hostmaster@energis-
ecs.com
7  c9.f.de.plusline.net (212.19.48.29) hostmaster@plusline.de
8  213.83.36.18 (213.83.36.18) hostmaster@plusline.de 158 ms 150 ms 150
ms
```

Aus diesen Angaben lassen sich insgesamt wenig Rückschlüsse auf den verwendeten Server ziehen. Lediglich der Hoster (plusline.de) und der Zonenverwalter (geumann.net) lassen sich erkennen. Ein Hinweis auf den zweiten Ki-ON-Server (213.83.36.19) wird nicht gegeben.

6.1.2 Betriebssystemerkennung

Die Verwendung von nmap (www.insecure.org) mit Host-Erkennung (Option -O) ergibt:

```
> nmap ... -O s1.ki-on.net

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host (213.83.36.18) appears to be up ... good.
...
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=796185 (Good luck!)

Sequence numbers: F6A0CA A7B4B2 E040A5 133878F 170509F 13ADF70
No OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
TSeq(Class=RI%gcd=1%SI=C29E9)
TSeq(Class=RI%gcd=1%SI=C2800)
TSeq(Class=RI%gcd=1%SI=C2619)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Ops=)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=Y%DF=Y%TOS=C0%IPLen=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E
)
```

Das verwendete Betriebssystem ist daraus zunächst nicht erkennbar; ein Vergleich mit entsprechenden Signaturen anderer Systeme lässt die Vermutung zu, dass es sich um ein Linux-System mit Kernel 2.4 handelt; für einen potenziellen Angreifer lässt sich damit jedoch keine gesicherte Aussage ableiten.

6.1.3 Sicherheitslücken

Um einen Überblick über die eventuell vorhandenen Sicherheitslücken des Servers zu erhalten, wurde eine Analyse mittels des Sicherheitsscanners Nessus (www.nessus.org) durchgeführt. Dabei wurde folgendes Ergebnis ermittelt (zusammengefasst):

```
Nessus Scan Report
Number of hosts which were alive during the test : 1
Number of security holes found : 1
Number of security warnings found : 2
Number of security notes found : 2
List of the tested hosts : s1.ki-on.net(Security holes found)
s1.ki-on.net :
List of open ports :
  ssh (22/tcp) (Security hole found)
  https (443/tcp) (Security warnings found)

Vulnerability found on port ssh (22/tcp)
You are running a version of SSH which is older than version 1.2.32, or a
version of OpenSSH which is older than 2.3.0. This version is vulnerable to
a flaw which allows an attacker to insert arbitrary commands in a ssh
stream.
Risk factor : High

Warning found on port https (443/tcp)
The Sambar webserver is running. It provides a webinterface for sending
emails.
...
Risk factor : High
-----
This file was generated by Nessus, the open-sourced security scanner.
```

Während die erste gemeldete Lücke tatsächlich ein Sicherheitsrisiko darstellt (siehe 6.4), handelt es sich bei der zweiten Warnung um eine Fehlmeldung.

Der vermeintlich identifizierte Sambar-Server ist auf dem Ki-ON-Linux-Server nicht vorhanden, dort läuft vielmehr ein Apache-Server. Sambar ist nur für Windows-Rechner verfügbar.

6.2 Firewall

Um die Qualität der Firewall zu überprüfen wurde mittels nmap ein Portscan auf die Server s1.ki-on.net sowie auf 213.83.36.19 durchgeführt. Dabei wurden verschiedene Scan-Methoden angewandt (TCP Connect [-sT], TCP SYN [-sS], Window Scan [-sW], UDP Scan [-sU]), um eine möglichst umfassende Aussage zu erhalten.

Insgesamt wurden folgende Ergebnisse erzielt (identisch für beide Server):

Protokoll	Port	Dienst
TCP	22	ssh
	443	https
UDP	kein offener Port gefunden	

Damit sind also nur diejenigen Ports von außen zugänglich, die zum Betrieb des Servers erforderlich sind. Eine weitere Einschränkung der Filterregeln ist auf dieser Ebene nicht erforderlich bzw. nicht sinnvoll.

6.3 Web-Server und SSL

6.3.1 Server-Identifizierung

Um die HTTP-Header des Web-Servers untersuchen zu können, wurde eine Perl-UserAgent-Verbindung über einen lokalen HTTPS-Proxy (DeleGate als HTTPS-zu-HTTP-Konverter konfiguriert) zum Ki-ON-Server hergestellt. Folgende Header-Information waren dabei erkennbar:

```
Response: 200 OK
Cache-Control: no-cache, must-revalidate
Date: Mon, 09 Jul 2001 15:43:38 GMT
Pragma: no-cache
Via: 1.1 - (DeleGate/7.3.4)
Server: Apache
Content-Language: de
Content-Length: 3027
Content-Type: text/html
Content-Type: text/html; charset=iso-8859-1
Expires: 0
Last-Modified: Mon, 09 Jul 2001 15:43:38 GMT
Client-Date: Mon, 09 Jul 2001 15:54:45 GMT
Client-Peer: 10.0.0.1:8080
DeleGate-Ver: 7.3.4 (delay=3)
Link: ; rel="stylesheet"; type="text/css"
Set-Cookie: SessionID=175903d404bcc68ff873918fb38cd316; path=/
Title: [KI-ON] - Anmeldung
X-Meta-Author: www.redlink.de
X-Meta-Robots: nofollow
```

Der Server identifiziert sich als Apache (ohne Versionsnummer). Da dies bereits einen möglichen Anhaltspunkt für die Ausnutzung von Schwachstellen bieten kann, sollte erwogen werden, keine oder eine andere Identifizierung zu verwenden.

6.3.2 Zertifikat

Die Eigenschaften des aktuell (Stand Ende Juli 2001) verwendeten SSL-Zertifikats lassen sich mittels entsprechender Prüfserver (warentest.de, netcraft.com und hisolutions.com) wie folgt erkennen:

Allgemein	RSA-Modulus:				1024
	Public	Exponent:			65537
	Seriennummer:	0x81cd3			
	Gültig ab:	Jul	16	13:32:23	2001 GMT
	Gültig bis:	Jul	16	13:32:23	2002 GMT
	Fingerprint:	15:4F:28:4D:F7:62:99:38:EE:9F:C2:07:DA:01:0B:C4			
Inhaber	CommonName:				s1.ki-on.net
	Land:	DE			
	Staat:				
	Ort:				Bremen
	Organisation:	REDLINK	Mediendienste		
	Organisationseinheit:	Ki-ON			
	E-Mail/URL:				
Herausgeber	CommonName:	Thawte	Server	CA	
	Land:	ZA			
	Staat:				
	Ort:	Cape	Town		
	Organisation:	Thawte	Consulting	cc	
	Organisationseinheit:	Certification	Services	Division	
	E-Mail/URL:	server-certs@thawte.com			

Hierbei handelt es sich also um ein Zertifikat, das von einer bekannten Zertifizierungsstelle (CA) ausgestellt wurde. Entsprechend wird dieses Zertifikat von den gängigen Browsern problemlos akzeptiert. Bei dieser CA handelt es sich allerdings nicht um eine Instanz, die im Rahmen des deutschen oder europäischen Signaturrechts arbeitet.

Obwohl im Ki-ON-Verfahren keine rechtsverbindlichen Handlungen im Sinne des Signaturgesetzes durchgeführt werden müssen, sollte erwogen werden, ob nicht zukünftig ein Zertifikat verwendet wird, das dem gesetzlichen Standard der fortgeschrittenen elektronischen Signatur genügt. Auf diese Weise kann einer eventuellen zukünftigen Anforderung in diese Richtung ohne nachträglichen Aufwand genügt werden.

Der ServerModulus und Exponent des Zertifikats sind mit 1024 bzw. 65537 Bit ausreichend groß, um einen Angriff durch Dritte zu verhindern.

6.3.3 Verschlüsselungsstärken

Um die SSL-Funktionalität des Servers zu testen, wurde mit einem entsprechend konfigurierbaren Browser (Opera 5) Verbindungsversuche mit verschiedenen fest eingestellten Verschlüsselungsstärken durchgeführt.

Der Server unterstützt sowohl SSL 2.0 als auch SSL 3.0 und TLS 1.0. Als Minimalverschlüsselung wird 40 Bit RC2 bzw. RC4 mit 512 bzw. 1024 Bit RSA und MD5 akzeptiert. Diese sog. Export-Verschlüsselung ist eine in ihrer Sicherheit künstlich reduzierte Variante, die es dem US-amerikanischen Geheimdienst ermöglichen soll, die verschlüsselte Verbindung mitzuhören. Als höchstmögliche Verschlüsselung wird 192 Bit 3DES mit 1024 Bit RSA und SHA angeboten. Dabei handelt es sich um eine Qualität, die nach aktuellem Kenntnisstand nicht gebrochen werden kann.

Um in allen Fällen eine hohe Verschlüsselungsqualität sicherzustellen, sollte der Server so eingestellt werden, dass er schwache Schlüssel nicht akzeptiert. Dies führt zwar ggf. dazu, dass auf Kundenseite eine Verbindung zum Ki-ON-Server nicht möglich ist, wenn dort ältere Browser zum Einsatz kommen. Andererseits wird dadurch an zentraler Stelle verhindert, dass im Einzelfall eine zu schwache Verschlüsselung verwendet wird und damit u.U. das Sicherheitsniveau der gesamten Anwendung gesenkt wird.

6.4 SSH

Eine Verbindung zum SSH-Port von s1.ki-on.net mit eingeschalteten Debug-Informationen ergibt folgendes Protokoll:

```
linux:~ # ssh -v s1.ki-on.net
SSH Version OpenSSH_2.3.0p1, protocol versions 1.5/2.0.
Compiled with SSL (0x0090600f).
debug: Reading configuration data /etc/ssh/ssh_config
debug: Seeding random number generator
debug: ssh_connect: getuid 0 geteuid 0 anon 0
debug: Connecting to s1.ki-on.net [213.83.36.18] port 22.
debug: Allocated local port 1023.
debug: Connection established.
debug: Remote protocol version 1.99, remote software version OpenSSH_2.1.1
debug: match: OpenSSH_2.1.1 pat ^OpenSSH[ _]2\.[012]
debug: Local version string SSH-1.5-OpenSSH_2.3.0p1
debug: Waiting for server public key.
debug: Received server public key (768 bits) and host key (1024 bits).The au-
thenticity of host 's1.ki-on.net' can't be established.
RSA key fingerprint is fa:37:91:56:1a:d2:58:52:ce:2e:6b:37:c9:c0:8e:2e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 's1.ki-on.net,213.83.36.18' (RSA) to the list of
known hosts.
debug: Seeding random number generator
debug: Encryption type: 3des
debug: Sent encrypted session key.
debug: Installing crc compensation attack detector.
debug: Received encrypted confirmation.
debug: Doing password authentication.
```

Daraus lässt sich die verwendete SSH-Implementierung (OpenSSH_2.1.1) erkennen sowie die verwendete Verschlüsselung (3DES). Während letztere als ausreichend sicher zu bewerten ist, handelt es sich bei der verwendeten SSH-Version um eine Implementation mit einer bekannten Sicherheitslücke, die es einem Angreifer durch Methoden des Stack-Overflow ermöglicht (siehe [Zalewski 2001]), beliebige Kommandos auf dem SSH-Server auszuführen und dadurch auch Superuser-Privilegien zu erhalten. Die Ausnutzung von Stack-Overflows ist eine weit

verbreitete Methode, um die Sicherheit von Rechnern zu beeinträchtigen; sie basiert auf einer unsauberen Programmierung im Zusammenhang mit Eingabepuffern fester Größe. Die Verwendung von Eingaben die länger als diese Puffer sind, kann dazu führen, dass diese Eingabe vom Betriebssystem als Maschinencode interpretiert und ausgeführt wird. Dadurch sind weitreichende Beeinträchtigungen des Systems durch die Benutzer möglich. Für Details dieser Methode siehe [A-leph 1996].

Um das Sicherheitsloch zu schließen, sollte auf Version 2.3.0 oder höher von OpenSSH gewechselt werden. Alternativ könnte die bestehende Version auch so konfiguriert werden, dass SSH Version 1 nicht unterstützt wird. Dadurch ließe sich das Problem ebenfalls umgehen, allerdings auf Kosten der Kompatibilität, da dann Clients, die nur SSH 1.x beherrschen, keine SSH-Verbindung mit dem Ki-ON-Server mehr aufnehmen können.

6.5 Benutzerauthentisierung

Um die Qualität der Benutzeranmeldung zu testen, wurde eine Reihe von künstlichen Fehlanmeldungen produziert. Dabei zeigt sich, dass Im Ki-ON-Verfahren offenbar keine Begrenzung hinsichtlich der Anzahl der Fehlanmeldungen bei einem Konto besteht. Entsprechend kann ein Angriber im Prinzip beliebig lange versuchen, eine gültige Kennung zu erraten, z.B. indem er gängige Kennwörter aus einem Wörterbuch verwendet. Der rechtmäßige Benutzer wird zudem nicht auf eventuelle Fehlanmeldungen seit dem letzten Zugriff hingewiesen.

Dies sollte so geändert werden, dass Konten nach einer bestimmten Anzahl von Fehlversuchen (z.B. 5) zumindest für einen gewissen Zeitraum (z.B. 30 Minuten) gesperrt werden. Dies ermöglicht zwar einen Angriff hinsichtlich der Verfügbarkeit, verbessert die Vertraulichkeit jedoch erheblich. Zudem sollte der Benutzer gewarnt werden, wenn Fehlanmeldungen an seinem Konto erfolgt sind.

Ein Probieren verschiedener Session-ID führte nicht zu einem erkennbaren Erfolg (d.h. ein Eindringen in fremde Sitzungen). Die ID sind ausreichend komplex aufgebaut, um ein Erraten nahezu unmöglich zu machen.

Die Verzögerung beim erfolglosen Login beträgt ca. 15 Sekunden; pro Tag sind daher über 5000 Versuche möglich; dies lässt sich durch parallele Zugriffe im Prinzip beliebig steigern. Ein Wörterbuch-basierter Angriff auf die Benutzerauthentisierung liegt daher im Bereich des Denkbaren, insbesondere dann, wenn eine Benutzerkennung bekannt ist. Die implementierte Verzögerung bietet daher einen gewissen Schutz, der gegenüber einer dynamischen Verzögerung oder einer befristeten Login-Sperre jedoch vergleichsweise gering ausfällt.

6.6 Terminalauthentisierung

Obwohl die Terminalidentifizierung mittels eines Cookies funktioniert, das bei jedem Zugriff auf den Ki-ON-Server an diesen übermittelt wird, zeigt sich, dass dieses Cookie nur zu Beginn ausgewertet wird. Ist anschließend eine Session-ID vergeben, genügt diese, um (auch bei fehlendem Cookie für die Terminalidentifizierung) eine Sitzung zu übernehmen.

Die Terminalauthentisierung sollte so gestaltet sein, dass die Identität des Terminals bei jedem Zugriff überprüft wird. Nur dadurch wird die Übernahme von aktiven Sitzungen durch Dritte tatsächlich erschwert.

6.7 Zugriffsschutz

Die dem Ki-ON-Verfahren zu Grunde liegenden Mechanismen ließen keine Schwächen hinsichtlich des Zugriffsschutzes angemeldeter Benutzer erkennen. Weder durch Variation der Session-ID noch durch den Aufruf besonderer URL (dazu wurde ein automatisiertes Werkzeug verwendet, das eine Reihe von speziellen URL aufruft, die zur Offenbarung interner Informationen wie Verzeichnislistungen führen können) war es möglich, auf Daten anderer Benutzer zuzugreifen, ohne zuvor eine Anmeldung unter deren Kennung zu unternehmen. Welche Möglichkeiten des Datenbankzugriffs bei einem Zugang, der nicht über den Web-Server abgewickelt wird, bestehen, konnte mit den verwendeten Methoden nicht ermittelt werden.

7 Ergebnisse und Empfehlungen

Insgesamt stellt das Verfahren Ki-ON eine weitgehend sichere Plattform zur Verarbeitung sensibler personenbezogener Daten dar. Die gleichwohl zur weiteren Verbesserung der Sicherheit erforderlichen Maßnahmen werden hier nochmals zusammengefasst:

- Es sollte eine eigenständige Firewall eingerichtet werden, die ausschließlich für diesen Zweck verwendet wird und keine nach außen gerichteten Serverdienste bereitstellt. Dabei sollte erwogen werden, ein anderes Betriebssystem als auf den Ki-ON-Servern zu verwenden. Dies bietet insofern einen Sicherheitsvorteil als ein Angreifer dann mit verschiedenen Systemen zu tun hat, die angegriffen werden müssen und einzelne Sicherheitslücken nicht durchgängig ausgenutzt werden können.
- Bestimmte SSL-Schlüssellängen sind darauf ausgelegt, Dritten die Entschlüsselung zu ermöglichen und können daher nicht als sicher gelten. Der Ki-ON-Server sollte daher Schlüssellängen unter 64 Bit nicht anbieten.
- Kennwörter müssen durch den Benutzer jederzeit änderbar sein und durch das System einer gewissen Verfallszeit unterworfen werden. Insgesamt wird eine Kennwortverwaltung empfohlen, die sich an den Maßstäben des BSI-Grundschutzkonzepts orientiert: Diese sollten nicht nur als organisatorische Vorgabe formuliert werden, sondern vom Ki-ON-System technisch erzwungen werden.
- Die Verwendung von Cookies zur Terminalidentifizierung stellt keine optimale Lösung dar. Da im Rahmen von Ki-ON auf die von SSL zur Verfügung gestellten Funktionalitäten zurückgegriffen werden kann, bietet es sich an, die dabei optionale Client-Authentisierung zu nutzen. Die zugelassenen Endgeräte müssen dazu mit einem Client-Zertifikat ausgestattet werden, das bei der Errichtung der SSL-Verbindung an den Server übermittelt wird. Dieser kann dann anhand des vorgelegten Zertifikats

überprüfen, ob sich das Endgerät im Kreis der zugelassenen Clients befindet und unbekannte Geräte bereits in dieser Phase abweisen.

- Der Server identifiziert sich als Apache (ohne Versionsnummer). Da dies bereits einen möglichen Anhaltspunkt für die Ausnutzung von Schwachstellen bieten kann, sollte erwogen werden, keine oder eine andere Identifizierung zu verwenden. Die Server-Identifizierung kann mittels Neukompilierung nach Änderung der Zeile

```
#define SERVER_BASEPRODUCT "Apache"
```

in der Datei "httpd.h" entsprechend geändert bzw. gelöscht werden.

- Obwohl im Ki-ON-Verfahren keine rechtsverbindlichen Handlungen im Sinne des Signaturgesetzes durchgeführt werden müssen, sollte erwogen werden, ob in Zukunft ein Zertifikat verwendet wird, das dem gesetzlichen Standard der fortgeschrittenen elektronischen Signatur genügt. Auf diese Weise kann einer eventuellen zukünftigen Anforderung in diese Richtung ohne nachträglichen Aufwand genügt werden.
- Eine Zertifizierungsstelle, deren Root-Zertifikat in Standard-Browsern enthalten ist, existiert zwar zurzeit noch nicht. Es wäre jedoch im Rahmen des Ki-ON-Verfahrens möglich, entsprechende Root-Zertifikate in die Browser zu integrieren. Im Zuge des geänderten Signaturgesetzes (SigG) ist allerdings zu erwarten, dass die Zahl der Anbieter deutlich zunehmen wird, die qualifizierte elektronische Signaturen nach § 2 SigG anbieten.
- Um in allen Fällen eine hohe Verschlüsselungsqualität sicherzustellen, sollte der Server so eingestellt werden, dass er schwache Schlüssel nicht akzeptiert. Dies führt zwar ggf. dazu, dass auf Kundenseite eine Verbindung zum Ki-ON-Server nicht möglich ist, wenn dort ältere Browser zum Einsatz kommen. Andererseits wird dadurch an zentraler Stelle verhindert, dass im Einzelfall eine zu schwache Verschlüsselung zum Einsatz kommt und damit u.U. das Sicherheitsniveau der gesamten Anwendung gesenkt wird.
- Um ein Sicherheitsloch im Zusammenhang mit SSH zu schließen, sollte auf Version 2.3.0 oder höher von OpenSSH gewechselt werden. Alternativ könnte die bestehende Version auch so konfiguriert werden, dass SSH Version 1 nicht unterstützt wird. Dadurch ließe sich das Problem ebenfalls umgehen, allerdings auf Kosten der Kompatibilität, da dann Clients, die nur SSH 1.x beherrschen, keine SSH-Verbindung mit dem Ki-ON-Server mehr aufnehmen können.
- Die Benutzerauthentisierung sollte so geändert werden, dass Konten nach einer bestimmten Anzahl von Fehlversuchen zumindest für einen gewissen Zeitraum gesperrt werden. Dies ermöglicht zwar einen Angriff hinsichtlich der Verfügbarkeit, verbessert die Vertraulichkeit jedoch erheblich. Zudem sollte der Benutzer gewarnt werden, wenn Fehlanmeldungen an seinem Konto erfolgt sind.
- Die Terminalauthentisierung sollte so gestaltet sein, dass die Identität des Terminals bei jedem Zugriff überprüft wird. Nur dadurch wird die Übernahme von aktiven Sitzungen durch Dritte tatsächlich erschwert.

Anlage zum Evaluierungsbericht

A Verfahrensänderungen

Aufgrund der Evaluierung wurden folgende Änderungen in Ki-ON durchgeführt:

1. **Passworte und Kontenverwaltung:**

Der Benutzer kann sein Passwort jederzeit selbst ändern. Dabei werden folgende Auflagen programmtechnisch durchgesetzt:

- Die minimale Passwortlänge beträgt 6 Zeichen.
- Die letzten 3 Passworte werden gespeichert und können nicht wieder verwendet werden. Das gleiche gilt für Passworte in umgekehrter Zeichenreihenfolge und sehr ähnliche Passworte.
- Das Passwort darf nicht in einer Liste von bekannten Worten enthalten sein.
- Das Passwort darf nicht 2 gleiche Zeichen hintereinander, 3 gleiche Zeichen an beliebigen Stellen im Passwort oder 3 Zeichen, die auf der Tastatur (QUERTZ oder QWERTY) hintereinander liegen, enthalten.
- Das Passwort darf nicht die Benutzerkennung, den Vor- oder den Nachnamen des Benutzers enthalten. Entsprechendes gilt für die umgekehrte Reihenfolge.
- Das Passwort muss mindestens eine Ziffer oder ein Sonderzeichen enthalten.
- Die maximale Gültigkeitsdauer beträgt 90 Tage.
- Benutzer müssen das Initialpasswort beim ersten Login ändern.
- Nach dem vierten erfolglosen Loginversuch wird der Account für 30 Minuten gesperrt.
- Nach einem erfolgreichen Login wird dem Benutzer der Zeitpunkt des letzten Logins und die Anzahl der erfolglosen Versuche angezeigt.

2. **OpenSSH:**

Auf dem Server wird jetzt die Version 2.5.2p2 verwendet.

3. **SSL_Schlüssellängen:**

Da die Deaktivierung von kurzen Schlüssellängen für HTTPS bedeuten würde, dass Benutzer mit älteren oder noch nicht entsprechend gepatchten Browsern keinen Zugriff mehr auf Ki-ON erhalten würden, werden kurze Schlüssellängen vom Apache-Server zwar akzeptiert, nachträglich aber über PHP abgefangen und mit einer Fehlermeldung die Verbindung beendet. Ansonsten entstünde der Eindruck, der Ki-ON-Server wäre vollständig ausgefallen.

4. Client-Zertifikate:

Um den Einsatz von Client-Zertifikaten für Ki-ON-Nutzer möglichst einfach zu gestalten, wird folgendes Verfahren umgesetzt:

- Liegt kein Client-Zertifikat vor, erhält der Benutzer nach erfolgreichem Login keinen Zugriff, sondern wird auf eine spezielle Seite umgeleitet.
- Dort kann er nach Eingabe eines weiteren Passworts (des bisherigen Terminal-Kennworts) ein Client-Zertifikat erstellen lassen, das direkt online heruntergeladen und in seinen Browser installiert wird.
- Das Terminal-Kennwort verliert hiernach seine Gültigkeit. Für ein weiteres Client-Zertifikat ist auch ein weiteres Passwort notwendig.
- Bei einigen Browsern (insbesondere Internet Explorer auf MacOS) ist ein solches Online-Verfahren nicht möglich. Hier wird ganz traditionell das Zertifikat per Post auf Diskette verschickt.

Literatur

[Aleph 1996]

Aleph One: Smashing The Stack For Fun And Profit, in: Phrack 49, 1996
(<http://www.phrack.org/show.php?p=49&a=14>)

[BSI]

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch
(<http://www.bsi.bund.de/gshb/deutsch/menue.htm>)

[BSI 2000]

Empfehlungen zum Schutz vor verteilten Denial of Service- Angriffen im Internet
(<http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=17&tdid=64&page=0>)

[Freier 1996]

Alan Freier, Philip Karlton, Paul Kocher: The SSL Protocol, Version 3.0, 1996

[Kühn/Schläger 1997]

Ulrich Kühn, Dr. Uwe Schläger: Datenschutz in vernetzten Computersystemen,
Datakontext, 1997

[Schmid 2000]

Egon Schmid (Hg.): PHP Handbuch, 2000 (<http://www.php.net/manual/de/>), dort:
Kapitel 4, Sicherheit

[Smith 1998]

Richard E. Smith: Internet-Kryptographie, Addison-Wesley, 1998

[Song 2000]

dsniff (<http://naughty.monkey.org/~dugsong/dsniff/>)

[Zalewski 2001]

Michael Zalewski: Remote vulnerability in SSH daemon crc32 compensation at-
tack detector (http://razor.bindview.com/publish/advisories/adv_ssh1crc.html)