VERSCHLÜSSELUNG: TRANSPARENT UND SICHER?

WIE TRANSPARENT DARF EINE SICHERE VERSCHLÜSSELUNG SEIN – WELCHE TRANSPARENZ IST FÜR DIE SICHERE VERWENDUNG DURCH DEN ANWENDER ERFORDERLICH?

Der Begriff Transparenz wird heute in zwei Richtungen verwendet: zum einen „ohne das Zutun eines Anwenders“ – also unsichtbar im Hintergrund – zum anderen „unter der vollständigen Veröffentlichung aller Details“, um alles sichtbar zu machen und keine Hintertüren oder verdeckte Kanäle zu ermöglichen. Im Zusammenhang mit der Verschlüsselung sensibler Daten ist also die Frage nicht nur, wie transparent die Verschlüsselung sein sollte, sondern auch welche Personengruppen welche Art der oben definierten Transparenz benötigen, um im Gesamtverfahren das gewünschte Maß an Sicherheit zu erreichen.

Am Beispiel gängiger Systeme zur Verschlüsselung möchten wir zuerst an Grenzwerten aufzeigen, wie wichtig die Diskussion für überall verfügbare Basistechnologien ist.

Beispiel 1: die Verschlüsselung von mobilen Datenträgern

Ein Anwender kopiert eine Präsentation auf einen Memory-Stick – die Verschlüsselung findet völlig transparent im Hintergrund statt. Der Anwender muss nun zumindest soweit informiert sein, dass er beurteilen kann, ob die Präsentation auf dem zur Präsentation vorgesehenen Drittrechner wieder entschlüsselt werden kann, ohne die Vertraulichkeit anderer Daten zu riskieren – insbesondere natürlich anderer Daten auf demselben Datenträger. Dass das nicht ganz trivial ist, zeigen mögliche Angriffe über USB-Dumper [1] sowie die Anforderungen an die Infrastruktur auf dem Drittrechner bei Verwendung einer PKI oder das Verständnis der benötigten Rechte auf dem Drittsystem zur Verwendung einer Anwendungs-Software oder eines Treibers zur Entschlüsselung.

Beispiel 2: Festplattenverschlüsselung

Festplattenverschlüsselungssysteme unterscheiden sich in vielen verschiedenen Facetten. Zum einen kann durch ein Pre-Boot-Authentication-Verfahren mit starker Authentisierung der Schutz der im Moment eines potentiellen Angriffs „ungenutzten Daten“ sichergestellt werden – z.B. bei Diebstahl oder Verlust von Gesamtsystemen wie Notebooks. Nach positiver Authentisierung des Anwenders stehen alle Daten auf der Festplatte aber jeder gestarteten Anwendung im Klartext zur Verfügung, da die Entschlüsselung „transparent“ im Hintergrund stattfindet. Entsprechend der Einschätzung von Microsoft [2] gehen jedoch mehr als 50% aller Gefährdungen von PCs und Notebooks von laufenden Anwendungen aus, die durch Schadcode infiltriert sind oder im laufenden Betrieb aus dem Internet oder durch infizierte Dokumente unerkannt verändert wurden. Sobald das Betriebssystem läuft, sind die sensiblen Daten auf der Platte also durch dieses Verfahren nicht mehr geschützt. Am anderen Ende der Sicherheitsskala gibt es Lösungen, mit welchen zwar alle Daten auf der Festplatte verschlüsselt sind, aber alle Schlüssel und Verfahren zur Entschlüsselung auf der Festplatte selbst untergebracht sind, wodurch auch Angriffe auf das „ruhende System“ einfacher werden. Der Besitzer eines Notebooks sollte hierüber zumindest soweit Bescheid wissen, dass er beurteilen kann, welche Sensitivitätsklassen er dem Notebook anvertrauen darf und wie gut er es in bestimmten Situationen durch physikalische Maßnahmen beschützen (lassen) muss. Der Sicherheitsverantwortliche und der Systembetreiber müssen sich einigen, ob sie für die Softwareverteilung und das Patch-Management Hintertüren offen lassen wollen, die natürlich das Gesamtsystem gefährden oder die Systems-Management-Verfahren komplexer oder sogar unmöglich machen.

Schon jetzt wird deutlich, dass unter dem Wunsch „alle Technik vor dem Anwender zu verbergen“ häufig ohne Not zu große Abstriche in der Sicherheit des Gesamtverfahrens gemacht werden. Aber auch die umgekehrte Richtung wird klar: es kann passieren, dass der Anwender in der Annahme, durch die Verschlüsselung vollständig geschützt zu sein, glaubt, auf andere wesentliche, ergänzende Verfahren verzichten zu können. Auch dieser wichtige Fall sei an einem Beispiel aufgezeigt.

Beispiel 3 - Selbstverschlüsselnde Hardware

Setzt ein Anwender für seine vertraulichsten Daten, z.B. zu geplanten Firmenübernahmen oder Personalentscheidungen, einen selbstverschlüsselnden Memory Stick ein, der ein beweisbar hohes Sicherheitsniveau (z.B. CC EAL 4+) erreicht, dann werden auf diesem Datenträger Daten zu unterschiedlichen Verwendungszwecken und unterschiedlicher Sensitivität gespeichert. Die Entschlüsselung der Daten findet dann auf jedem beliebigen System „transparent im Hintergrund“ sofort nach Einstecken und Eingabe der richtigen PIN oder positiver Authentisierung des Fingerabdrucks statt – unabhängig davon, welches Programm auf diese Daten zugreift. Der Anwender glaubt nun auf einem Fremdrechner nur seine mitgebrachte Präsentation oder ein bestimmtes Angebot zu öffnen, real werden aber von einem lesehungrigen Hintergrundprogramm alle Daten des Datenträgers ausgelesen – dank der Transparenz der Entschlüsselung im Klartext und ohne das Wissen des Anwenders. Diese Art der Schadprogramme wird „USB-Dumper“ [1]

genannt – das Prinzip findet man aber auch in verschiedenen anderen Angriffsmustern wieder.

Eine andere, wieder zweischneidige Herausforderung bei der Verschlüsselung von Nutzdaten erleben wir bei der sicheren Übertragung von Daten ins Internet.

Beispiel 4 – Verschlüsselter Upload ins Internet

Jeder Anwender kann sich privat seinen eigenen Speicherplatz für wenig Geld im Internet mieten und den Zugang zu diesem Speicherplatz einer automatischen Verschlüsselung unterwerfen. Zum einen gibt es nun natürlich die fehlerhafte Annahme, diese Daten wären aufgrund der verschlüsselten Übertragung auch geschützt gespeichert. Zum anderen besteht aber aus Firmensicht folgende Problematik: die verschlüsselte Übertragung der Daten kann zwar technisch auf der Firewall des Unternehmens „aufgebrochen“ werden, diese Maßnahme ist aber in vielen Fällen in Deutschland rechtlich nicht zulässig. Dadurch bietet sich eine Möglichkeit für Innentäter oder auch für eingeschleusten Schadcode Daten nach draußen zu schleusen, ohne dass die Inhalte erkannt werden. Statistische Daten über das ausgetauschte Datenvolumen erzeugen zwar eventuell Verdachtsmomente, sind aber als Beweislage nicht ausreichend, so dass es sich für den Schutz vor Wirtschaftsspionage in DLP-Projekten [3] empfiehlt, die Datenkontrolle bei den „unverschlüsselten“ Zugriffen - also auf dem Client - durchzuführen und den Upload von verschlüsselten Dateien zu verhindern.
Stellt man allen Anwendern in der Annahme Gutes zu tun eine starke Verschlüsselung zur freien Verfügung, kann man bei dem nächsten Audit eines Wirtschaftsprüfers ein böses Erwachen erleben.

Beispiel 5 – Verschlüsselung und Langzeitarchivierung

Entsprechend GoBS, GoS, FAIT und vielen anderen Auflagen und Standards unterliegen bestimmte Daten – z.B. Daten zur Rechnungslegung – einer Archivierungspflicht. Die Archivierungspflicht ist nur erfüllt, wenn die archivierten Daten über den Verpflichtungszeitraum auch im Klartext zur Verfügung stehen. Hat nun ein Anwender die Möglichkeit die unter Archivierungspflicht liegenden Daten verschlüsselt abzulegen, dann sind die Daten zwar archiviert, aber die gesetzliche Auflage ist nicht erfüllt. Diese Herausforderung lässt sich nur durch eine geeignete Schlüsselhinterlegung lösen. Die Aufbewahrungspflicht der beteiligten Schlüssel UND des gesamten Verfahrens zur Entschlüsselung sind also ebenfalls an die gesetzlichen Auflagen gekoppelt. Damit der Wirtschaftsprüfer das Verfahren auch abnimmt muss dieses also nicht nur „transparent“ sein sondern auch jede Nutzung der optionalen Verschlüsselung daraufhin überprüft werden, ob archivierungspflichtige Daten betroffen sind und dann sofort eine geeignete Maßnahme getroffen werden.

Verschlüsselung: transparent UND sicher?

Hat man also Geld in Form von Lizenzen, Hardware oder internen Ressourcen ausgegeben, um die Sicherheit zu erhöhen, gilt es einiges zu berücksichtigen:

1. Die technischen Möglichkeiten zur Nutzung der Verschlüsselung können entweder
    a. optional zur Nutzung zur Verfügung gestellt werden, oder
    b. erzwungen werden – entlang der Vertraulichkeit des Inhalts, des Speicherortes z.B. mobiler Datenträger, des Anwenders...
    c. an manchen Stellen müssen sie verboten werden.
2. Der Einsatz ist so zu organisieren, dass die Sicherheitsfunktionen
    a. immer wenn notwendig Verwendung finden und
    b. der Anwender bei der Nutzung
        i. nicht nur weiß wie die Verschlüsselung zu verwenden ist, sondern
        ii. auch sichergestellt ist, dass er versteht in welchen Fällen an welchen Orten er wieder unter welchen Umständen entschlüsseln kann.
    c. bei rechtlicher Notwendigkeit wieder aufgehoben werden können.
3. Die Sicherheit des Verfahrens erfüllt auch in den realen Nutzungsszenarien der Anwender immer die vorgegebenen Sicherheitsziele.
4. Die Möglichkeit der Wahl von persönlichen Schlüsseln darf den Help Desk nicht belasten.

Bei der Diskussion der Transparenz der Verschlüsselung muss natürlich noch darauf hingewiesen werden, dass das Verschlüsselungsverfahren selbst gegenüber den IT-Sicherheitsbeauftragten und Entscheidern offengelegt – also transparent – sein muss und die Verwendung der Schlüssel nachvollziehbar und geschützt sein muss.

Best Practice und CheckListen

Einige Tipps aus der Praxis erleichtern den Umgang mit dem Schlagwort „Transparenz“ bei der Projektierung und bei der Lösungsauswahl, geben Indikatoren für sichere Handlungsanweisungen und Abgrenzungen zu Nutzungsszenarien, die nicht zu empfehlen sind.

Transportverschlüsselung optional oder erzwungen?

Die Daten unterwegs stellen häufig ein hohes Risiko dar, da Memory-Sticks leicht verloren gehen können und nach dem novellierten Datenschutzgesetz bei bestimmten Daten, die sich im Klartext auf dem verlorenen Stick befinden, eine sehr unangenehme Handlungsnotwendigkeit mit öffentlicher Informationspflicht entstehen kann. Die Haftung geht nach KonTraG direkt in den Vorstand oder die Geschäftsführung. In den seltensten Fällen denken Anwender in der Hektik des Alltags daran sensible Daten besonders zu behandeln. Deshalb sind Verfahren, die eine optionale Verschlüsselung so verstecken, dass der Anwender einen anderen Knopf drücken (z.B. sicher speichern) oder ein eigenes Menü (z.B. Kontextmenü mit verschlüsseln) öffnen muss hier nur die zweite Wahl. Gut ist es, wenn die Verschlüsselung als administrative Option je nach dem verwendeten Datenträger,

dem Anwender und den zu speichernden Inhalten in der Sicherheitsrichtlinie als „zwangsweise“ oder „optional“ gesetzt werden kann. Da es häufig berechtigte Anwender gibt, die Daten auch im Klartext exportieren dürfen, kann in diesen Fällen das Speichern einer elektronischen Willenserklärung sinnvoll sein, um den Haftungsübergang in Echtzeit zu dokumentieren.

Die verschiedenen Datenverluste z.B. von Call Centern haben in der letzten Zeit die Aufmerksamkeit geschärft. Immer wenn man mit Aushilfskräften oder vorübergehend Beschäftigten auf „teuren“ Datenbeständen aus dem eigenen Haus oder den Daten der Kunden operiert, kann ein geeigneter „Bindungsbereich“ der Schlüssel die gewünschte Verfahrenssicherheit ergeben. Unternehmensschlüssel sind dem Anwender und Administrator nicht bekannt und schützen vor der Datenmitnahme nach Haus oder dem Verkauf an Dritte, erlauben aber trotzdem den Austausch von sensiblen Daten im Unternehmen oder mit definierten Partnern und Kunden.
Nimmt der Anwender Daten mit, die er mit einem persönlichen Schlüssel oder unter Verwendung einer PKI verschlüsselt hat, dann ist es wichtig alle benötigten Anwendungen auf den Datenträger aufzubringen und den Anwender zu informieren, welche Anforderungen er an ein Drittsystem stellen muss, um dort die Daten sicher einzulesen. Da solche Security Awareness-Maßnahmen immer zeitgleich mit der Verwendung gekoppelt sein müssen und nie überhand nehmen dürfen oder komplexe Sachverhalte beschreiben können, sollte hier also auf Verfahren zurückgegriffen werden, die keine Voraussatzungen an das Drittsystem stellen.

Je nach der Vertrauenswürdigkeit der Anwendergruppen, der behandelten Daten, der verwendeten mobilen Datenträger, der verwendeten Kommunikationsanwendungen (Browser, ftp, Mail ...) und der gewünschten Haftungssituation empfiehlt es sich folgende Fragen zu klären:

- Wie kann die Security Awareness in Echtzeit „themenaffin“ entsprechend der unterstützten Nutzungsszenarien jeweils aktuell an die Gesetzes- und Compliance-Lage kommuniziert werden?
- Soll in bestimmten Fällen der Haftungsdurchgriff in den Vorstand nach KonTraG durch eine revisionssichere elektronische Willenserklärung gebrochen werden?
- Gegen welche Angriffe wollen Sie schützen und wer kann diese Angriffe durchführen?
- Wie schützen Sie das vertrauliche Material bei transparenter Entschlüsselung vor dem Zugriff nichtberechtigter Anwendungen?
- Wie können Sie mit unterschiedlichen Schlüsselsystemen die Ziele der DLP-Projekte unterstützen? Bei Bedarf auch mandantenfähig für einzelne Abteilungen – z.B. Personal, Betriebsrat, Vorstand ...
- Wie können die gesetzlichen und innerbetrieblichen Auflagen – auch die Kostenreduktion des Help Desks – an eine Archivierung und Backup-Recovery durch Schlüsselhinterlegung und die Verfügbarkeit der Verfahren abgebildet werden?
- Wie kann die Komplexitätsvorgabe bei persönlichen Schlüsseln benutzerfreundlich und ohne Help Desk-Aktivität durchgeführt werden?
- Wie können Trivialdaten, z.B. Wegbeschreibungen o.ä. von einer Zwangsverschlüsselung ausgenommen werden und in Koexistenz zum verschlüsselten Datenmaterial unverschlüsselt, z. B. auf mobilen Datenträgern, gespeichert werden?

Verschlüsselung: transparent UND sicher?

- Wie kann sichergestellt werden, dass eine gestohlene Festplatte nur den Hardwarewert aber keinen Informationswert beim Verkauf auf dem Schwarzmarkt erzielt?
- Wodurch wird sichergestellt, dass der Anwender unter Zeitdruck keine „Extraaktion“ durchführen muss, die er evtl. vergessen kann?
- Wie kann Backup-Recovery evtl. sogar dezentral für den Außendienst geleistet werden, ohne die Vertraulichkeit zu gefährden?
- Wie können selbstverschlüsselnde Verfahren von einer Zwangsverschlüsselung ausgenommen werden?
- Wie können Spezialverfahren, die keine verschlüsselten Inhalte akzeptieren, mit den Verschlüsselungsverfahren zusammen arbeiten?
- Entsprechen die verwendeten Algorithmen, die Lagerung der Schlüssel und das Gesamtverfahren dem angestrebten Sicherheitslevel?

Literaturverzeichnis:

[1] BSI, IT-Grundschutzkatalog, G5.142
[2] Microsoft, Microsoft Security Intelligence Report Volume 8, S.81
[3] Peter Gola (2010), Datenschutz und Multimedia am Arbeitsplatz, Datakontext, S. 197ff.

Informieren Sie sich im Detail über unsere Innovationen und kontaktieren Sie uns unter:

Info@itWatch.de oder 089/ 620 30 100.

itWatch GmbH

Aschauer Str. 30
D-81549 München