



Verschlüsselung

Orientierungshilfe

So erreichen Sie den Landesbeauftragter für den Datenschutz Niedersachsen:

Schreiben Postfach 221, 30002 Hannover
Anrufen 0511 / 120-4500
Faxen 0511 / 120-4599
E-Mailen poststelle@lfd.niedersachsen.de
Surfen www.lfd.niedersachsen.de
Persönlich Brühlstraße 9, Hannover

Hinweise zur Verschlüsselung

Erforderlichkeit

Werden Informationen elektronisch übertragen, besteht die Möglichkeit, dass diese Unbefugten zur Kenntnis gelangen, von diesen manipuliert oder durch technische Fehler verändert werden. Gleiches gilt auch bei der Speicherung von Daten auf elektronischen Datenträgern, insbesondere wenn diese transportiert werden.

Wirksamstes Mittel gegen diese Gefahren ist der Einsatz von Verschlüsselungstechnik. Bei der Verschlüsselung (Kryptographie) werden die zu schützenden Daten so verändert, dass sie nur autorisierten Personen oder Geräten verständlich sind, für alle anderen aber sinnlos erscheinen. Grundprinzip ist die Veränderung (Vertauschung und Ersetzung) der Daten mit Hilfe eines Verschlüsselungsalgorithmus, der durch einen Parameter (Schlüssel) gesteuert wird. Wem Algorithmus und Schlüssel zur Verfügung stehen, kann die Daten ver- bzw. entschlüsseln. Ohne Kenntnis des Schlüssels lassen sich die Daten im Grunde nur durch Ausprobieren aller möglichen Schlüssel zurückgewinnen („brute force–Attacke“).

Empfehlung

Personenbezogene Daten sollten grundsätzlich bei der Übertragung über öffentliche Leitungen verschlüsselt werden. Da häufig nicht abschätzbar ist, wie sensitiv zu übertragende Daten sind, sollte die Verschlüsselung als Grundschutzmaßnahme bei allen Weitverkehrsnetzen (insbesondere im Internet) eingesetzt werden. Bei der Speicherung von personenbezogenen Daten auf Systemen oder Datenträgern, die besonderen Gefährdungen unterliegen (z.B. bei Laptops und ungesichertem Datenträgertransport) ist eine Verschlüsselung vorzunehmen.

Verschlüsselungsalgorithmen

Die Stärke eines Verschlüsselungsverfahrens richtet sich nach dem Aufwand, der für eine Entschlüsselung ohne Kenntnis des Schlüssels notwendig ist. Er hängt in erster Linie von der Qualität des Algorithmus, von der Schlüssellänge und von der zur Verfügung stehenden Rechnerkapazität ab. Da sich die Rechnerkapazitäten durch den technologischen Fortschritt ständig vergrößern, müssen Schlüssellänge oder Algorithmus im Lauf der Zeit ebenfalls erweitert bzw. verbessert werden, um eine ausreichende Stärke des Verfahrens zu gewährleisten.

Bei den Verschlüsselungsalgorithmen unterscheidet man die **symmetrische Verschlüsselung** (gleicher Schlüssel zum Verschlüsseln und Entschlüsseln) und die **asymmetrische Verschlüsselung** (unterschiedliche Schlüssel zum Verschlüsseln und zum Entschlüsseln). Die bekanntesten Algorithmen sind

- **DES** (data encryption standard) ist ein symmetrischer Verschlüsselungsalgorithmus, der 1977 als US-Verschlüsselungsstandard genormt wurde. Er ist allgemein bekannt, vielfach getestet und als starker Algorithmus anerkannt. Wenn bei Verfahren mit DES allerdings kurze Schlüssel eingesetzt werden, sind die Chiffre vergleichsweise leicht zu entschlüsseln. Schlüssellängen von 40 bit bieten daher nur eine eingeschränkte Sicherheit. Auch Schlüssel mit 56 bit lassen sich mit entsprechendem Aufwand zeitnah „knacken“. Zur Zeit sollten Schlüssellängen von möglichst 128 bit eingesetzt werden. Eine Weiterentwicklung des DES ist der **Triple-DES**, bei dem der DES-Algorithmus drei mal durchlaufen wird. Zurzeit sucht das US-amerikanische National Institute of Standards and Technology (NIST) nach einem Nachfolger für DES. Hierfür stehen verschiedene Algorithmen zur Auswahl. Der neue Standard soll den Namen **AES** (advanced encryption standard) erhalten.
- **IDEA** (international data encryption algorithm) ist ebenfalls ein anerkannter symmetrischer Verschlüsselungsalgorithmus. Er wurde von L. L. Massey und X. Lai an der ETH Zürich entwickelt und

1990 veröffentlicht. Er ist schnell und steht in seiner Qualität nicht hinter DES zurück, wird häufig sogar als stärker eingeschätzt. Die übliche Schlüssellänge für IDEA beträgt 128 bit.

- **RSA** (Rivest Shamir Adleman) ist ein nach seinen Erfindern benannter asymmetrischer Verschlüsselungsalgorithmus. Auch RSA ist allgemein bekannt, vielfach getestet und als starker Algorithmus anerkannt. Die Schlüssellänge sollte mindestens 1024 bit betragen.

Weitere bekannte Algorithmen sind z.B. Blowfish, RC4, RC5, Diffie-Hellmann oder MD5. Die Algorithmen, ihre Stärken und Schwächen sowie ihre Einsatzmöglichkeiten sind in der Fachliteratur ausführlich beschrieben.

Verschlüsselungsverfahren zur Sicherung der Vertraulichkeit

Die Auswahl des geeigneten Verschlüsselungsverfahrens hängt vom Einsatzbereich ab. Man unterscheidet:

- **Verschlüsselte Datenspeicherung**

Verschlüsselung bei der Speicherung von Daten auf einem Datenträger, z.B. der Festplatte des Rechners. Diese Maßnahme soll verhindern, dass Unbefugte durch den Zugriff auf einen Rechner oder durch das Entwenden von Datenträgern personenbezogene Daten lesen oder manipulieren.

- **Leitungsverschlüsselung**

Verschlüsselung von Daten, die über eine Leitung übertragen werden. Diese Maßnahme schützt gegen das unbefugte Lesen oder Manipulieren von Daten während der Übertragung durch das "Anzapfen" der Leitung. In den Rechnern und Verbindungen außerhalb des Leitungsbereichs liegen die Daten allerdings im Klartext vor. Die Leitungsverschlüsselung ist z.B. bei der Datenübertragung zwischen zwei gesicherten lokalen Netzen über eine öffentliche Leitung sinnvoll.

- **Ende-zu-Ende-Verschlüsselung**

Verschlüsselung von Daten auf der gesamten Übertragungstrecke zwischen dem Absender und dem Empfänger. Diese Maßnahme schützt gegen das unbefugte Lesen oder Manipulieren von Daten auf der gesamten Übertragungstrecke. Bei der Ende-zu-Ende-Verschlüsselung werden nur die Inhaltsdaten, nicht aber die Verbindungsdaten verschlüsselt.

Für die verschlüsselte Datenspeicherung werden im allgemeinen die auf symmetrischen Algorithmen beruhende **private key** – Verfahren eingesetzt. Die Ver- und Entschlüsselung der Daten erfolgt z.B. transparent bei jedem schreibenden bzw. lesenden Zugriff auf die Festplatte mit Hilfe einer Zusatzkarte im PC. Viele einfachere Verfahren beruhen auf Software-Lösungen, die aus der Anwendung heraus standardmäßig oder nutzerabhängig Daten, etwa Textdokumente, vor der Speicherung verschlüsseln und beim erneuten Aufrufen entschlüsseln. Die so verschlüsselten Daten können auch gesichert an Empfänger übertragen werden. Mit allen Empfängern muss allerdings vorher ein gesicherter Schlüsselaustausch stattgefunden haben. Dies ist nur praktikabel, wenn die Empfängergruppe klein bleibt.

Für die Datenübertragung insbesondere in großen Teilnehmergruppen werden auf asymmetrischen Algorithmen beruhende **public key** - Verfahren verwendet. Hierbei wird für jeden Nutzer ein Schlüssel zum Verschlüsseln erzeugt und allen anderen Nutzern zur Verfügung gestellt. Mit diesem „öffentlichen Schlüssel“ verschlüsselte Daten können nur mit dem dazu gehörigen geheimen Schlüssel des Empfängers gelesen werden. Um den Aufwand bei den langsamen asymmetrischen Algorithmen gering zu halten, setzen die meisten public-key-Verfahren **Hybrid-Techniken** ein, bei denen für jede Übertragung nur ein sogenannter session key asymmetrisch verschlüsselt wird, die eigentlichen Daten aber mit Hilfe des session keys symmetrisch verschlüsselt werden. Bei diesem Verfahren hängt die Sicherheit von beiden verwendeten Algorithmen und Schlüssellängen ab.

Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, müssen das IuK-System des Absenders und des Empfängers den Zugriffsschutz auf das Verschlüsselungsprogramm und die Schlüssel ausreichend gewährleisten. Hierfür ist es in vielen Fällen erforderlich, ein Chipkartensystem aufzubauen und die Schlüssel auf den Chipkarten zu speichern.

Ein Sonderfall der verschlüsselten Datenspeicherung stellt die Passwortverschlüsselung dar. Um ein Passwortverfahren ausreichend sicher zu gestalten, müssen die Passwörter mit einer **Einwegverschlüsselung** verschlüsselt werden. Dieses Verfahren hat den Vorteil, dass einmal verschlüsselte Passwörter niemand im Klartext lesen kann. Der Rechner kann dennoch das Passwort bei erneuter Eingabe verschlüsseln und durch Vergleich mit dem bereits gespeicherten Chiffretext dessen Korrektheit überprüfen.

Digitale Signaturen für die Sicherung von Integrität und Authentizität

Die Datenverschlüsselung bietet einen sehr hohen Vertraulichkeitsschutz, sie sichert aber nur begrenzt die Integrität der Daten und führt zumindest bei public key - Verfahren zu keinem Schutz der Authentizität des Absenders. Integrität und Authentizität lassen sich jedoch mit digitalen Signaturverfahren sichern. Bei diesen Verfahren werden beim Absender eine Art Quersumme, der Hash-Wert, aus den zu signierenden Daten gebildet. Der Hash-Wert wird mit einem public key – Verfahren verschlüsselt, wobei hier der Schlüssel zum Verschlüsseln geheim gehalten wird. Der Empfänger entschlüsselt den Hash-Wert mit dem zum Absender gehörenden öffentlichen Schlüssel und bildet selbst aus den empfangenen Daten den Hash-Wert. Sind beide Hash-Werte gleich, so sind Integrität und Authentizität nachgewiesen. Voraussetzung hierfür ist allerdings, dass der Empfänger den öffentlichen Schlüssel des Absenders von einer Stelle erhält, der er vertrauen kann. Für ein digitales Signaturverfahren ist deshalb eine vertrauenswürdige Stelle für die Schlüsselverwaltung, ein „**Trust Center**“, erforderlich.

Die Verwendung einer digitalen Signatur ist erforderlich, wenn elektronische Dokumente für rechtsverbindliche Vorgänge verwendet werden oder Daten in vernetzten Systemen verarbeitet werden und der Verlust der Integrität oder Authentizität dieser Daten erhebliche Gefahren für die Betroffenen auslösen würden. Aber auch bei weniger sensiblen Daten, etwa bei der Vorgangsbearbeitung, beim allgemeinen E-Mail-Verkehr oder beim Datenträgeraustausch, empfiehlt sich das Signaturverfahren, um so die Revisionsfähigkeit zu sichern.

Mit dem Signaturgesetz (SigG; Art. 3 des Informations- und Kommunikationsdienste-Gesetz (IuKDG) vom 28.07.1997; BGBl. S. 1870) wird ein sicheres Signaturverfahren beschrieben. Bei Einführung und Einsatz von Signaturverfahren sind die Anforderungen des SigG zu beachten. Informationen zum SigG, der SigVO und zu den Maßnahmekatalogen für Zertifizierungsstellen nach dem SigG können u.a. bei der Regulierungsbehörde für Telekommunikation und Post (www.regtp.de) eingeholt werden.

Verschlüsselungsprodukte

Auf dem Hard- und Software-Markt sind eine Vielzahl von Verschlüsselungsprodukten verfügbar. Sie sind zum Teil bereits in Betriebssystemen oder Anwendungen enthalten, der überwiegende Teil ist jedoch spezielle Sicherheits-Software, die zusätzlich zum Betriebssystem oder zur Anwendung beschafft werden muss. Zu beachten ist, dass Verschlüsselungsprogramme aus den USA aufgrund der dortigen Exportbeschränkungen oft nur mit sehr kurzen Schlüssellängen geliefert werden.

U.a. folgende Verschlüsselungsprodukte sind von besonderer Bedeutung:

- **PGP** (Pretty Good Privacy) ist ein Public-Domain-Verschlüsselungsprogramm mit Hybrid-Technik, das auf den Algorithmen RSA (für das Schlüsselmanagement) und IDEA (zur Datenverschlüsse-

lung) basiert. Mit PGP können Nachrichten verschlüsselt und mit einer digitalen Signatur versehen werden. PGP steht im Internet unter verschiedenen Adressen zum Herunterladen zur Verfügung.

- In Unix-Systemen steht grundsätzlich das Verschlüsselungsprogramm **crypt** zur Verfügung, oft ist dieses allerdings wegen der Exportbeschränkungen der USA entfernt worden.
- Für den E-Mail-Verkehr stehen eine Reihe von Produkten zur Verfügung, die nach dem **Mail-Trust**-Standard des deutschen Teletrust e.V. verschlüsseln und untereinander kompatibel sind.
- Ein weiterer E-Mail-Verschlüsselungsstandard ist die „Secure Multipurpose Internet Mail Extension“ (**S/MIME**), entwickelt von RSA Data Securities. Er wird u.a. von Lotus, Microsoft und Banyan verwendet.
- Für Datenübertragungen mit TCP/IP (z.B. im Internet) kann das Sicherheitsprotokoll **SSL** (Secure Socket Layer) verwendet werden, dass von den gängigen Internet-Browsern unterstützt wird.
- Alle neueren Betriebssysteme enthalten eine Einwegverschlüsselung für das jeweilige **Passwortverfahren**. In den meisten neuen Netzwerkbetriebssystemen werden Passwörter nur verschlüsselt im Netz übertragen.

Viele Firmen bieten für die verschiedensten Bereiche Verschlüsselungsprodukte an. Für die öffentliche Verwaltung stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Offline-Verschlüsselungsprogramm (MIC 7.0) für den Einsatz auf stationären und tragbaren PC unter gewissen Randbedingungen zur Verfügung.

Checkliste

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen

- **Erfüllt**
- **Nicht erfüllt**
- **Trifft nicht zu.**

Diese Basisantworten können im Bedarfsfall durch kurze Erläuterungen in dem Feld Bemerkungstext ergänzt werden. Auf diese Weise liegt nach Abarbeitung der Checkliste eine übersichtliche Aufstellung der noch zu treffenden Maßnahmen vor.

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher ist die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich zu behandeln!

Checkliste Verschlüsselung

Klassifizierung der Schutzstufe			ggf. Begründung der Einstufung (Extrablatt)	
Stufe A	Stufe B	Stufe C	Stufe D	Stufe E

(Erläuterungen zum Schutzstufenkonzept siehe Anhang)

Bereich, in dem ein Verschlüsselungs- bzw. Signaturverfahren eingesetzt ist:		
Einsatzbereich 1:	Verschlüsselungsprodukt:	Schlüssellänge:
Einsatzbereich 2:	Verschlüsselungsprodukt:	Schlüssellänge:
Einsatzbereich 3:	Verschlüsselungsprodukt:	Schlüssellänge:

1	Einsatzbereiche von Verschlüsselungs- und Signaturverfahren	Erfüllt			
		Nicht erfüllt			
		Trifft nicht zu			
		Bemerkungstext			
In folgenden Fällen wird eine Verschlüsselung vorgenommen:					
1.1.	Bei der Übertragung von Daten der Stufe D oder E über Weitverkehrsnetze (nach Möglichkeit bei allen personenbezogenen Daten).				
1.2.	Bei der Übertragung von Daten ab der Stufe C in Netzen, die öffentlich zugänglich sind, insbesondere im Internet.				
1.3.	Bei der Speicherung von Daten ab der Stufe C auf Systemen oder Datenträgern, die besonderen Gefährdungen unterliegen (z.B. bei Laptops, ungesichertem Datenträgertransport).				

1.4.	Bei der Speicherung von Passwörtern.				
1.5.	Bei der Fernübertragung von Administrator-Passwörtern.				

In folgenden Fällen wird ein Signaturverfahren gemäß Signaturgesetz verwendet:					
1.6.	Bei Verwendung von elektronischen Dokumenten für rechtsverbindliche Vorgänge.				
1.7.	Bei Verarbeitung von Daten in vernetzten Systemen (z.B. bei Vorgangsbearbeitung, E-Mail-Verkehr, Datenträgeraustausch), die bezüglich der Integrität oder Authentizität den Stufen D oder E zuzuordnen sind (nach Möglichkeit auch bei weniger sensitiven Daten).				

2.	Gestaltung und Durchführung der Verschlüsselungsverfahren	Erfüllt			
		Nicht erfüllt			
		Trifft nicht zu			
		Bemerkungstext			
2.1.	In allen oben aufgeführten Bereichen ist eine Soft- oder Hardware im Einsatz, die eine Verschlüsselung mit einem starken Algorithmus (z.B. Triple-DES, IDEA, DES, RSA) ermöglicht.				
2.2.	Es ist technisch oder organisatorisch sicher gestellt, dass die Verschlüsselung in allen relevanten Fällen zum Einsatz kommt.				
2.3.	Die verwendete Schlüssellänge lässt eine Entschlüsselung nur mit einem unverhältnismäßig hohen Aufwand zu.				
2.4.	Die geheimen Schlüssel werden bei den Nutzern getrennt vom Rechner und Verschlüsselungsprogramm gesichert aufbewahrt (z.B. auf Chipkarten). Die Schlüsselabfrage erfolgt elektronisch zusammen mit der Abfrage eines Passwortes oder einer PIN.				

2.	Gestaltung und Durchführung der Verschlüsselungsverfahren	Erfüllt			
		Nicht erfüllt			
		Trifft nicht zu			
					Bemerkungstext
2.5.	Die Schlüsselgenerierung und-verwaltung wird von zuverlässigen Personen durchgeführt. Befugnisse und Aufgaben sind in einer Dienst- oder Arbeitsanweisung bzw. vertraglich festgehalten.				
2.6.	Eine Schlüsselübergabe an neue Nutzer erfolgt nur, wenn deren Authentizität und Berechtigung nachgewiesen sind.				
2.7.	Die Schlüssel werden in regelmäßigen Zeitabständen geändert und gesichert übergeben.				
2.8.	Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter geschützt.				
2.9.	Die Nutzer der Verfahren sind ausreichend in deren Umgang geschult und auf Gefahren hingewiesen worden.				

Anhang: Schutzstufenkonzept

Personenbezogene Daten werden nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange bei Mißbrauch dieser Daten in 5 Schutzstufen untergliedert. Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. Die Betrachtung ist vielmehr auf die gesamte Datei, ggf. auf die gesamte DV-Anlage auszudehnen. Werden personenbezogene Daten unter einem Auswahlkriterium in eine Datei aufgenommen, das in der Datei nicht enthalten ist, so ist dieses Auswahlkriterium bei der Klassifizierung mit zu bewerten. Enthalten Dateien umfassende Angaben zu einer Person (Dossiers), so sind sie in eine höhere Schutzstufe einzuordnen, als dies nach den Einzeldaten erforderlich wäre. Es werden folgende Schutzstufen unterschieden:

- Stufe A: Frei zugängliche Daten, in die Einsicht gewährt wird, ohne daß der Einsichtnehmende ein berechtigtes Interesse geltend machen muß, z.B. Adreßbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken.
- Stufe B: Personenbezogene Daten, deren Mißbrauch zwar keine besondere Beeinträchtigung erwarten läßt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen.
- Stufe C: Personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann ("Ansehen"), z.B. Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.
- Stufe D: Personenbezogene Daten, deren Mißbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann ("Existenz"), z.B. Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Konkurse.
- Stufe E: Daten, deren Mißbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

Falls die Sensitivität nicht bekannt ist, ist von der höchsten Sensitivitätsstufe auszugehen. Denkbar ist auch, daß der Schutz empfindlicher Firmendaten ohne Personenbezug die Einstufung bestimmt.