Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Verschlüsselung

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

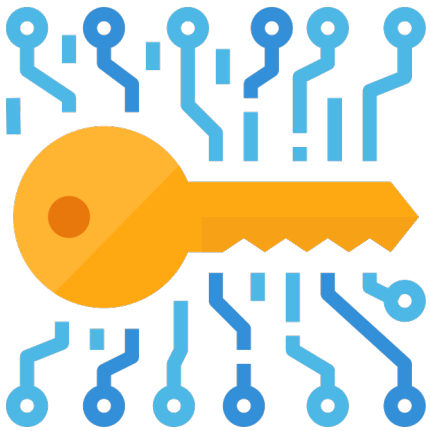
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Verschlüsselung – Was ist das?

Verschlüsselung ist ein **Prozess**, bei dem Daten so umgewandelt werden, dass sie unlesbar und unverständlich für nicht leseberechtigte Dritte werden. Der Hauptzweck der Verschlüsselung besteht darin, die Vertraulichkeit von Informationen zu gewährleisten, indem nur **berechtigten Empfängern** der Zugriff auf diese ermöglicht wird. Der Prozess, diese Daten wieder in das ursprüngliche lesbare Format umzuwandeln, wird als Entschlüsselung bezeichnet.



Welche Maßnahmen sind erforderlich?

Unternehmen und Institutionen haben verschiedene Möglichkeiten, ihre Daten und Kommunikationsmittel durch Verschlüsselung zu schützen. Eine der gängigen Maßnahmen ist der **Einsatz von kryptografischen Algorithmen und Protokollen**, um Daten zu verschlüsseln. Diese werden auch in standardisierter Verschlüsselungssoftware verwendet, um Daten auf Festplatten, externen Speichermedien oder in der Cloud zu verschlüsseln. Die **Verschlüsselung von E-Mails**, insbesondere deren Anhängen, und Instant-Messaging-Diensten sollte ebenfalls sichergestellt werden, um eine vertrauliche Kommunikation zu gewährleisten.

Der Austausch von Daten über das Internet oder im internen Netzwerk birgt das Risiko, dass diese von Angreifern abgefangen und mitgelesen werden. Aus diesem Grund ist es wichtig, die Netzwerkkommunikation mit **Verschlüsselungs-zertifikaten wie SSL oder TLS** abzusichern. Im Zugriff auf das Internet mit dem Browser sollte stets darauf geachtet werden, dass die Verbindung zur Website verschlüsselt über das **Protokoll HTTPS** erfolgt.

Die Einführung einer Verschlüsselung in einem Unternehmen oder einer Institution erfordert eine sorgfältige Planung und Umsetzung. Zunächst sollten die **Anforderungen und Risiken analysiert** werden, indem die wichtigsten Daten und Kommunikationskanäle, die Schutz benötigen, identifiziert und potenzielle Risiken und Bedrohungen bewertet werden. Auf Basis dieser Analyse sollten die ausgewählt werden. **geeigneten Verschlüsselungsmethoden und -technologien** Um ein hohes Maß an Sicherheitsbewusstsein zu gewährleisten, ist die **Schulung der Mitarbeiter** in der Verwendung der Verschlüsselungstechniken von großer Bedeutung. Schließlich sollten Unternehmen und Institutionen regelmäßig die **Wirksamkeit** der Verschlüsselungsmaßnahmen überwachen und diese bei Bedarf anpassen, um einen optimalen Schutz ihrer Daten und Kommunikation sicherzustellen.

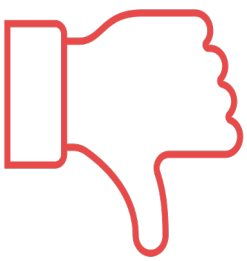
Cyber-Sicherheitsrat Deutschland e.V.

Welche Chancen gibt es?

Die Verwendung von Verschlüsselung bietet Unternehmen und Institutionen viele Chancen und Vorteile. Sie ermöglicht den **Schutz sensibler Daten vor unbefugtem Zugriff oder Manipulation** und sichert die **Privatsphäre** von Kunden, Mitarbeitern und Partnern. Im Falle eines Diebstahls von Daten sind diese auch außerhalb der Geschäftsräume vor Zugriff auf die Dateninhalte durch Verschlüsselung geschützt. Darüber hinaus hilft sie bei der **Einhaltung gesetzlicher Vorschriften** und branchenspezifischer Datenschutzanforderungen.
Verschlüsselung trägt auch zur **Verbesserung des Vertrauens** und der Glaubwürdigkeit gegenüber Kunden und Geschäftspartnern bei und vermeidet finanzielle Verluste sowie Reputationsschäden durch **Datenschutzverletzungen**.

Welche Risiken gibt es?

Allerdings gibt es auch einige Risiken und Nachteile bei der Verwendung von Verschlüsselung. Ein wesentlicher Aspekt ist die **Komplexität** der Verschlüsselungssysteme, die teilweise eine sorgfältige Verwaltung erfordern, um effektiv zu funktionieren. **Leistungsprobleme** können ebenfalls auftreten, da Verschlüsselung zu einer Verlangsamung von Systemen und Netzwerken führen kann, insbesondere bei ressourcenintensiven Verschlüsselungsmethoden.
Die **Verwaltung der Schlüssel** ist eine weitere Herausforderung, denn der Verlust oder die Kompromittierung von Schlüsseln kann zu einem **unwiederbringlichen Datenverlust** führen.
Ferner führt der **Verlust des Schlüssels** der zur Entschlüsselung der Dateien benötigt wird dazu, dass diese Daten nicht mehr zu entschlüsseln sind. Ransomwareangriffe machen sich diesen Umstand zunutze und verschlüsseln die Daten des Opfers und verkaufen dann den Schlüssel zur Entschlüsselung der Daten für ein hohes Lösegeld an das Opfer des Angriffs.



Cyber-Sicherheitsrat Deutschland e.V.

Wem nutzt Verschlüsselung?

Verschlüsselungsmaßnahmen richten sich an **unterschiedliche Zielgruppen** innerhalb eines Unternehmens oder einer Institution und erfordern eine enge Zusammenarbeit zwischen diesen Gruppen. Die Geschäftsführung und **Entscheidungsträger** müssen die Bedeutung der Verschlüsselung erkennen und Ressourcen für deren Implementierung bereitstellen. Dies stellt sicher, dass die **IT-Abteilungen** in der Lage sind, die Auswahl, Implementierung und Verwaltung von Verschlüsselungslösungen erfolgreich durchzuführen. **Mitarbeiter** spielen ebenfalls eine wichtige Rolle im Umgang mit Verschlüsselung. Sie müssen geschult und sensibilisiert werden, um Verschlüsselungstechnologien sicher und effektiv einzusetzen.

Darüber hinaus ist es wichtig, auch **Kunden und Geschäftspartner** in den Verschlüsselungsprozess einzubeziehen. Indem sie über die Sicherheitsmaßnahmen informiert werden, wird das **Vertrauen in die Kommunikation** und den Datenaustausch aufgebaut und gestärkt. Dies fördert eine sicherere und vertrauenswürdigere Zusammenarbeit zwischen den beteiligten Parteien.

Fazit

Verschlüsselung ist ein **unverzichtbares Sicherheitsinstrument** für Unternehmen und Institutionen, um sensible Daten und Kommunikation vor unbefugtem Zugriff zu schützen.

Durch die Implementierung geeigneter Verschlüsselungsmaßnahmen können Organisationen das **Risiko von Datenschutzverletzungen minimieren**, die **Privatsphäre** von Kunden und Mitarbeitern wahren und **gesetzliche Anforderungen erfüllen**.

Trotz einiger Risiken und Nachteile ist der Nutzen der Verschlüsselung in der heutigen zunehmend vernetzten und datengetriebenen Welt von großer Bedeutung. Durch eine sorgfältige **Planung, Implementierung und Verwaltung von Verschlüsselungsmaßnahmen** können Organisationen den Schutz ihrer Informationen und die Sicherheit ihrer Systeme langfristig gewährleisten.

Cyber-Sicherheitsrat Deutschland e.V.