Allianz für Cyber-Sicherheit

EMPFEHLUNG: IT IM UNTERNEHMEN

Schutz vor Ausspähung

1 Ausgangslage

Mit den im Folgenden dargestellten Maßnahmen zum Schutz vor Ausspähung richten sich die Mitglieder des Expertenkreises Cyber-Sicherheit[1] an Unternehmen mit dem Ziel, das Risiko einer Ausspähung zu minimieren, indem Maßnahmen der Cyber-Sicherheit[2] mit pragmatischen Vorschlägen zu deren Umsetzung konkretisiert werden.

Die Sicherheit der eingesetzten Informationstechnik ist als zentrale geschäftsunterstützende Funktion zu betrachten, denn mit steigender Durchdringung des Wirtschaftsgeschehens mit IT-Systemen aller Art geht ein Wandel weg von der Devise *„der Große gewinnt“* hin zur Devise *„der Schnelle und gut informierte gewinnt“* einher. Aktuelle und nicht öffentlich zugängliche kritische Daten, die Kronjuwelen eines Unternehmens, sind daher mit einem erheblichen wirtschaftlichen Vorteil verbunden.

2 Konsequenzen für den Schutz von Informationen

Eine gute Faustregel lautet: **5 Prozent der im Unternehmen vorhandenen Informationen bilden diese Kronjuwelen**. Verteidigen Sie diese Informationen im höchsten Maße und schützen Sie die restliche IT mit Standard-Schutzmaßnahmen. Um sich vor Ausspähung effektiv zu schützen und Angriffe abzuwehren, sind Prävention, Detektion und Reaktion von entscheidender Bedeutung. Grundvoraussetzung ist dabei immer der Einsatz vertrauenswürdiger Informationstechnik.

2.1 Motivation und Risiken des Angreifers

Angreifer verfolgen eine Vielzahl von Zielen, wie Ausspähung, Sabotage oder das Erbeuten finanzieller Mittel. Eine frühe Aufdeckung eines Angriffs stellt jedoch für jeden Angreifer das größte Risiko mit für ihn folgenschweren Konsequenzen dar. Ziele des Verteidigers sollten demnach neben der Vermeidung eines Datenabflusses und der Verringerung der Angriffsfläche stets die **Erhöhung des Aufdeckungsrisikos und Aufwands** für den Angreifer sein.

2.2 Präventive, detektive und reaktive Maßnahmen

Konkret können Sie dies mit Schutzmaßnahmen für Prävention (wie Schwachstellen-Management, ISMS), Detektion/Abwehr (wie Antivirensoftware, Firewalls, IDS/IPS oder Endpoint-Security Lösungen) und Reaktion (wie ein Backup-Konzept, IT-forensische Methoden) umsetzen. Etablieren Sie im gesamten Netzwerk eine ausreichende Aufklä-

1 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Erfahrungsaustausch/Expertenkreise/Cyber-Sicherheit/expertenkreis_cybersicherheit.html
2 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_006.html

rung (z. B. Security-Monitoring, Baselining), um Angriffe zu erkennen und das Aufdeckungsrisiko für den Angreifer signifikant zu erhöhen. Für fortgeschrittene Angriffe können automatisierte IT-Systeme nur eine unterstützende Funktion einnehmen. Für die Analyse der gesammelten Daten ist dabei geeignetes Personal mit ausreichender Expertise einzusetzen. Durch Verschlüsselung steigt zudem der Aufwand für Angreifer, abgegriffene Daten weiter zu verwerten, signifikant.

3 Grundlagen vertrauenswürdiger Informationstechnik für den Schutz Ihrer Daten

Gefährdungen der Vertraulichkeit, aber darüber hinaus auch der Verfügbarkeit und der Integrität von Unternehmensdaten kann mit folgenden konkreten Maßnahmen umfassend entgegengewirkt werden:

- Ausschließlicher Einsatz von Produkten solcher Hersteller, denen im nationalen und internationalen Rahmen ein ausreichendes Vertrauen entgegengebracht werden kann, unter Vermeidung von Abhängigkeiten zu nur einem Unternehmen (Dual-/Multi-Vendor-Strategie)
- Sicherstellen, dass ein Hersteller IT-Sicherheitsfunktionen anbietet, die Erkennungen von Integritätsverletzungen eines IT-Systems erleichtern (z. B. Einsatz von Whitelisting-Mechanismen, Definition erlaubter Verhaltensweisen über Mandatory Access Control sowie Logging)
- Einfordern und Prüfen der Dokumentation aller Funktionen, die die IT-Sicherheit der eingesetzten Systeme oder der übertragenen oder verarbeiteten Daten betreffen, und idealerweise Einsatz quell-offener Produkte unter freien Lizenzen
- Prüfung bei der Auswahl von Produkten, ob nachvollziehbare Zusicherungen des Herstellers vorliegen, dass die Produkte frei sind von undokumentierten Funktionen und entsprechende Rücktrittsrechte oder Nachbesserungsverpflichtungen eingefordert werden können; der Hersteller sollte zudem darstellen, welche eigenen Anstrengungen er zur Aufdeckung von Hintertüren oder bewusst platzierten Schwachstellen unternimmt, und diese Darstellung veröffentlichen
- Einfordern von Informationen zum kompletten Produktionsprozess vom Hersteller, einschließlich aller Zulieferungen; speziell muss dabei die Integrität der gesamten Produktionskette nachvollziehbar dargestellt werden
- Einsatz von speziell abgesicherten Fernwartungszugängen und One-Way-Gateways
- Sicherstellen, dass der Hersteller schnell auf bekannt gewordene Sicherheitslücken reagiert, indem er Informationen zu Schwachstellen und Aktualisierungen kurzfristig zur Verfügung stellt; die daraus gewonnenen Erkenntnisse zu Angriffsmustern und aktuellen Vorfällen sollten unmittelbar zur Detektion ergänzt werden
- Nutzung sicherer und überprüfter Implementierungen von kryptographischen Mechanismen auf Grundlage von herstellerunabhängigen Vorgaben und Zertifizierungen
- Verschlüsselte und zugriffsgeschützte Datenablage (insbesondere auch beim Schutz von Kundendaten sowie zur Minimierung von Haftungsrisiken und Reputationsschäden)
- Plus: Zusatzmaßnahmen bei höherer Cyber-Sicherheits-Exposition (wie im Kapitel „Zusatzmaßnahmen bei höherer Cyber-Sicherheits-Exposition“ in den „Basismaßnahmen der Cyber-Sicherheit“ dargestellt)

Eine dauerhafte Sicherstellung dieser Grundlage ist zum Schutz der von Ihnen identifizierten Kronjuwelen Ihres Unternehmens zwingend notwendig. Die regelmäßige Prüfung der IT-Systeme und Schulung des verantwortlichen Personals durch Dritte sind daher empfehlenswert.

4 Schutz der Kommunikation durch Verschlüsselung

Neben den Maßnahmen zum Schutz von Informationen sollte darüber hinaus als präventive Sicherung Ihrer Kommunikation stets ein Ziel im Vordergrund stehen: **Verschlüsseln Sie Ihre Kommunikation – immer!** Konkret bedeutet das im Falle von E-Mail den Einsatz von PGP und S/MIME sowie Server-zu-Server-Verschlüsselung. Eine durchgehende Verwendung von SSL/TLS und VPN-Lösungen ist zudem umzusetzen. Grundsätzlich wird empfohlen, dabei nur solche Kryptographie einzusetzen, die auf dem aktuellen Stand der Technik ist. Im Detail können die Anforderungen an Algorithmen und Schlüssellängen der Technischen Richtlinie TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[3] des BSI entnommen werden. Für Informationen zu sicheren kryptographischen Verfahren kann neben den Technischen Richtlinien auch auf den Algorithmenkatalog[4] der Signaturverordnung (SigV) zum deutschen Signaturgesetz (SigG) zurückgegriffen werden. Die erreichbare Schutzwirkung wird in diesen Dokumenten detailliert beschrieben.

5 Fazit

Für die verlässliche Gewährleistung der klassischen Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität soll neben den beschriebenen Schutzmaßnahmen auch Verschlüsselung – wo immer möglich – eingesetzt werden. **Wenn jeder seine Daten angemessen schützt und Kommunikation immer verschlüsselt, werden mögliche Angreifer gezwungen, deutlich mehr Zeit und Energie aufzuwenden, um Daten zu erbeuten und diese zu entschlüsseln.** Da bei allen Angreifern Zeit und Energie endlich sind, ist bei durchgehender Verschlüsselung eine massenhafte Ausspähung nicht mehr möglich. Dadurch wird die Gefahr einer erfolgreichen Ausspähungen insgesamt deutlich minimiert.

6 Links

Zusammenfassende Übersicht über die im Text referenzierten Quellen:

1. Expertenkreis Cyber-Sicherheit des BSI
   https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Erfahrungsaustausch/Expertenkreise_/Cyber-Sicherheit/expertenkreis_cybersicherheit.html
2. Basismaßnahmen der Cyber-Sicherheit
   https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_006.html
3. BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
   https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
4. Kryptoalgorithmen https://www.bsi.bund.de/Algorithmenkatalog

Dieses Dokument wurde durch den „Expertenkreis Cyber-Sicherheit des BSI“ erstellt, dem neben Vertretern des Bundesamtes für Sicherheit in der Informationstechnik auch Mitarbeiter anderer Unternehmen angehören. Weitere Informationen finden Sie unter: www.allianz-fuer-cybersicherheit.de

Kommentare und Hinweise zu diesem Dokument können von Lesern an **info@cyber-allianz.de** gesendet werden.

3 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
4 https://www.bsi.bund.de/Algorithmenkatalog.html