Datensicherheit mit Konzept

Mattias Ruchhöft Computer und Arbeit 11/2019 Ab Seite 31

IT-SICHERHEITSSYSTEME Viele Systeme, die der IT-und Datensicherheit dienen, basieren auf einer totalen Verhaltenskontrolle der Nutzer. Wie sicher sind also die Beschäftigten?

DARUM GEHT ES

1. Täglich gibt es neue Meldungen zu Datenverlusten oder Betrügereien, die mittels IT-Systemen begangen werden.

2. Unternehmen versuchen häufig, sich durch Software zu schützen.

3. Gremien sollten auf ein ganzheitliches Schutzkonzept drängen, das Schulungen der Belegschaft enthält.

Die umfangreichen Möglichkeiten zur Leistungs- und Verhaltenskontrolle von Sicherheitssystemen sind ein wichtiges Thema für Betriebs- und Personalräte. Ist das Thema IT-und Datensicherheit durch den Schutz vor Leistungs- und Verhaltenskontrolle aber bereits erschöpft? Wie sieht es aus mit Schulungen, in denen die Kolleginnen und Kollegen lernen, wie sie tendenziell bedrohliche Dinge wie z. B. Schad-Mails erkennen können? Im Sinne des bestmöglichen Schutzes der Beschäftigten gilt es für die Gremien, ein ganzheitliches Vorgehen der Betriebe im Bereich der Datensicherheit zu fordern und zu fördern.

Welche Bedrohungen gibt es?

Um eine sichere Datenverarbeitung zu gewährleisten, ist die Bedrohungslage zu analysieren, der ein Konzern, eine Behörde oder ein Unternehmen ausgesetzt ist. Dazu gehören z. B. die folgenden Szenarien, die dafür sorgen können, dass Daten verlorengehen oder unbefugten Dritten in die Hände fallen:

- Es gibt Schadprogramme, die u. a. über Spam-Mails oder das Herunterladen von Anwendungen aus dem Netz verteilt werden und Daten abfließen lassen können.
- Seit einigen Jahren existieren sogenannte Botnetze; das ist der Zusammenschluss von Geräten, z. B. um gezielt massenhafte Anfragen an Server zu versenden. Diese Art des Angriffs wird auch DDoS-Attacke genannt, und soll gezielt Systemabstürze herbeiführen. DDoS steht für »Distributed-Denial-of-Service-attack« und bedeutet wörtlich übersetzt »verteilte Verweigerung des Dienstes Angriff«. In der Vergangenheit waren durch solche Attacken namhafte Unternehmen – wie z. B. Amazon in den USA – teilweise über Stunden nicht erreichbar.
- Das sogenannte »Social Engineering« ist eine Methode, die auf eine zwischenmenschliche Beeinflussung abzielt, um Personen zur Preisgabe von vertraulichen Informationen zu bringen. Dieses Risiko ist nicht durch eine Software abzustellen, sondern nur durch Information und Training der Beschäftigten.
- Bei einer sogenannten Manin-the-Middle-Attacke steht der Angreifer in der Mitte zwischen zwei Kommunikationspartnern in einem Netzwerk. Dadurch kann dieser Angreifer, der beiden Partnern vortäuscht, er wäre das jeweilige Gegenüber, alle Informationen des Datenaustausches abgreifen und für sich nutzen. Der Angreifer hat auch die Möglichkeit, falsche Informationen weiterzugeben, da er das Netzwerk kontrolliert.
- In den letzten Jahren haben Angriffe auf Netzwerke mit sensiblen Daten – z. B. von Behörden – von sich reden gemacht, wie z. B. die Attacke auf das Netzwerk des Bundestags, die lange unentdeckt blieb. Hierbei handelt es sich um Advanced Persistent Th-reats (APT), zu Deutsch: fortgeschrittene, andauernde Bedrohung. Bei der Nutzung von Datenträgern stellen Diebstahl oder Verlust ein hohes Risiko dar.

Eine Bedrohung ist letztlich auch das Verhalten von Mitarbeiterinnen und Mitarbeitern im öffentlichen Raum. Wer regelmäßig mit der Deutschen Bahn fährt bekommt viele sogenannte Unternehmensgeheimnisse wie Entwicklungen, Erfindungen, Personal- oder Bewerbungsgespräche mit, da diese laut in einen Großraumwagen besprochen werden. Das kann nur durch Schulungen und andere Maßnahmen eingegrenzt werden.

SCHULUNG

Social Engineering – ein wichtiges Schulungsthema

Beispiel für eine relativ einfache Maßnahme: Ein Mann mit einer DHL-Uniform kommt mit einer Sackkarre, vollbeladen mit Paketen, und steht vor dem Nebeneingang der Firma, wo auch ein Häuschen für die Raucher steht. Eine freundliche Kollegin oder ein freundlicher Kollege macht dem Paketboten die Tür zum Nebeneingang auf. Eine alltägliche Situation – nur hat der Mann seine DHL-Uniform bei eBay für 15 Euro erstanden und den Transporter bei Hertz gemietet, aber noch nie bei der DHL gearbeitet. Nun ist er in der Firma und kann im Gebäude

vertrauliche Informationen sammeln. Viele Unternehmen und Behörden werden für solche einfachen Fälle bereits eine Regelung haben. Dennoch ist das Thema Sicherheitskonzept immer auch eine Frage der Qualifizierung. Betriebs- und Personalräte haben hier Mitbestimmungsrechte und können sich entsprechend einmischen. Wenn durch so eine Szene ein Schaden eintritt, wird die oder der Betroffene gegebenenfalls abgemahnt oder entlassen – ob sie oder er vorher geschult wurde oder nicht. Es gilt also, die Risikominimierung für die Beschäftigten aktiv mitzugestalten.

Was leisten IT-Sicherheitsanwendungen?

Der Markt von IT-Werkzeugen zur Erhöhung der Sicherheit ist ähnlich unübersichtlich wie der Markt für Mobiltelefone. Es ergibt daher wenig Sinn, hier auf einzelne Produkte einzugehen. Wir werfen daher einen Blick auf die typischen Elemente von IT-Sicherheitspaketen. Dazu gehören Virenscanner, Netzwerkabsicherungen und sogenannte Endpoint-Controls, also die Absicherung der Endgeräte der Beschäftigten. Diese Anwendungen scannen die Handlungen der Nutzer im Netzwerk oder am Rechner nach auffälligen Verhaltensweisen oder unüblichem Datenverkehr.

Datenverluste können durch spezielle Anwendungen verhindert werden (sogenannte Data Loss Prevention). Für bestimmte Informationstypen (z. B. Unternehmensgeheimnisse) werden durch Verschlüsselungstechniken oder das Unterbinden bestimmter Handlungen, wie das Kopieren oder Mailen an externe Adressen, Datenverlusten vorgebeugt. Das klingt zwar sinnvoll, durch die Überwachung des Netzwerkverkehrs in den Softwarelösungen entsteht aber auch ein lückenloses Bild der Tätigkeiten der Kolleginnen und Kollegen, die die IT des Unternehmens oder der Behörde nutzen. Damit ist eine umfangreiche Leistungs- und Verhaltenskontrolle möglich. Diese muss auf den Zweck des ordnungsgemäßen Betriebs der Systeme durch die zuständigen Administratoren eingeschränkt werden. Es muss auch geregelt werden, was passiert, wenn beispielsweise eine Alarmmeldung in einem der Sicherheitssysteme aufpoppt, die einzelne Beschäftigte betreffen. Besteht dann ein Risiko für diese Person oder geht es nur um eine Korrektur der Einstellungen? Für die Verarbeitung solcher Alarmmeldungen sollten Bestimmungen getroffen werden – sei es in einer Rahmen-Vereinbarung oder in einer konkreten Dienst- oder Betriebsvereinbarung zu den Sicherheitssystemen. Sicherheitsanwendungen beinhalten auch Funktionen, die über das reine Überwachen hinausgehen, so z. B. das Wiederherstellen gelöschter Dateien auf Endgeräten oder das Sammeln von Informationen, Dokumenten und Dateien für Compliance-Untersuchungen. Solche Funktionen sind gesondert zu betrachten und zu regeln. Was geschieht in einem Verdachtsfall? Wer stößt eine Untersuchung an? Wer darf diese ausführen? Wer informiert wen und wann? Und wann werden der Personal- oder Betriebsrat und der betriebliche Datenschutzbeauftragte informiert? Diese Fragestellungen sollten einer Vereinbarung beantwortet sein.

IT-Grundschutz-Konzept

IT-Sicherheitsanwendungen allein genügen anhand der vielfältigen Bedrohung nicht, um ein hinreichendes Maß an Datensicherheit zu erlangen.

Die Herangehensweise beim Erarbeiten oder Prüfen eines IT-Schutz-Konzepts lässt sich gut anhand des IT-Grundschutzmodells des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nachvollziehen.

Dieses nennt als Grundlage zunächst die übergreifenden Sicherheitsaspekte, wie beispielsweise das allgemeine Sicherheitsmanagement und dessen Organisation, das Datensicherungskonzept und den Schutz vor Schadprogrammen. Anschließend sind die IT-Infrastruktur wie Gebäude, Rechenzentren und die einzelnen Arbeitsplätze zu prüfen. Auch die Einstellungen und das Zusammenwirken der einzelnen IT-Systeme gehören zum Grundschutzmodell und umfassen die Sicherheitsaspekte sowohl von Clients als auch von Servern.

Nach der Analyse der IT-Systeme folgen Vernetzungsaspekte, die zum Beispiel das Netzmanagement, WLAN oder die VPN -Verbindung (Virtual Private Network – Sicherheitstunnel für Zugriffe von außen) umfassen. Die eigentlichen Anwendungen, wie Webserver, Faxserver oder Datenbanken, sind abschließend ebenfalls zu betrachten.

Die Maßnahmen des IT-Grundschutzes sollten zu einem kompletten Sicherheitskonzept gebündelt werden und Einstellungen in Systemen, den Einsatz von IT-Sicherheitssystemen, Anweisungen, Schulungen und Informationen umfassen.

Empfehlenswert ist auch eine Datenklassifizierung, die die Geheimhaltungsstufen und Maßnahmen zum Schutz kritischer Informationen enthält. Daraus leiten sich wiederum die Einstellungen zum Schutz vor Datenverlusten ab, die in den Systemen hinterlegt werden können (Anwendungen zur Data Loss Prevention).

Gremien sollten sich einmischen

Die beschriebene Betrachtung vom allgemeinen zum speziellen gehört in ein Gesamtkonzept zur IT- und Datensicherheit in Unternehmen wie Behörden und geht über die Nutzung einzelner Softwareprodukte weit hinaus. Interessenvertretungen sollten nach solchen Sicherheitskonzepten und den Auswirkungen auf die Beschäftigten im Sinne der Kontrolle ihrer Tätigkeiten durch Software und Schulungen (siehe den Kasten auf Seite 32) fragen – und diese dann auch entsprechend mitbestimmen und regeln. Machen Sie sich und Ihrem Arbeitgeber klar: Ein Sicherheitskonzept ist nur so gut, wie die Menschen, die es umsetzen sollen. Es gehört mehr dazu als ein Virenscanner oder ein E-Learning, das die Kolleginnen und Kollegen nebenbei in 30 Minuten durchklicken müssen.

Ein tolles Beispiel

Das Beispiel eines guten Sicherheitskonzepts soll diese Ausführungen abschließen. In unserem Beispiel-Konzern hat der Bereich IT-Sicherheit neben der Ausstattung mit Virenscannern, Netzwerkanalysen und Endpointcontrols ein umfangreiches Sicherheitskonzept erarbeitet, das bei den einzelnen Mitarbeitern ansetzt. Als Leitfragen dienten hierzu:

- Wie wird gearbeitet?

- Wo wird gearbeitet?
- Wie kommt das Thema Sicherheit in die Köpfe?

Die Antwort auf die letzte Frage ist einleuchtend: durch Betroffenheit! Dazu wurde ein Informations- und Schulungskonzept erarbeitet, das in Stufen ausgerollt werden soll. Startpunkt war eine kleine Informationskampagne mit Plakaten, kurzen Videos und Dokumenten zum Thema Datenschutz am Arbeitsplatz und unterwegs sowie Informationen darüber, wie einzelne Beschäftigte eine Spam-Mail erkennen können.

Darauf aufbauend werden weitere Themen hinzukommen – begleitet durch Anweisungen, Anregungen und Schulungen. Der Konzernbetriebsrat und die örtlichen Betriebsräte der einzelnen Gesellschaften sind von Anfang an involviert, um die Informationsmaßnahmen so zu gestalten, dass sie bei den Kolleginnen und Kollegen auch wirklich ankommen.

Das Konzept ist mit dem Konzernbetriebsrat vereinbart worden und die IT-Anwendungen sind in einer ergänzenden Vereinbarung zur vorhandenen umfangreichen IT-Rahmen-Konzernbetriebsvereinbarung mit Zuständigkeiten, Berechtigungen und Informationswegen bei Untersuchungen geregelt. So geht es auch!

SEMINAR ZUM THEMA +

Mattias Ruchhöft, Technologieberater bei der dtb Kassel, info@dtb-kassel.dewww.dtb-kassel.de

– Datenschutz