IT-SICHERHEITSKONZEPTE

Wirksam und preiswert – wie geht das?

Wirksame IT-Sicherheitskonzepte müssen nicht kostenintensiv sein. Die folgenden sieben Schritte können der Führungsebene in Kommunalverwaltungen und kommunalen Unternehmen helfen, einen passenden und wirtschaftlichen Ansatz für Ihre IT-Sicherheit zu finden.

#1 Bewertung Schadenspotenzial

Im ersten Schritt wird die Bedeutung der IT-Sicherheit für Ihre Organisation identifiziert. Alle Unternehmen und Institutionen sind permanent im Visier von Angreifern. Bei „Streu-Angriffen“ versucht ein Angreifer auf möglichst einfache Weise Systeme zu kapern, um diese für seine Zwecke zu missbrauchen oder Erpressungen durchzuführen. Gezielte Angriffe erfordern wesentlich mehr Aufwand und werden dort stattfinden, wo ein sehr lukrativer Vorteil zu erzielen ist.

Zu Beginn einer IT-Sicherheitskonzeption sollte also geklärt werden, ob es datentechnische Kronjuwelen gibt. Nehmen Sie zunächst eine grobe Abschätzung des Schadenspotenzials für diese vor: Mit welchen Kosten müssen Sie rechnen, wenn Anwendung X für einen Tag nicht zur Verfügung steht? Wie hoch wäre der Aufwand, wenn die Systeme kompromittiert wurden und neu aufgesetzt werden müssen? Welcher Schaden entsteht, wenn jemand vertrauliche Informationen abzieht und diese weiter gibt? Gibt es Kunden oder Partner, die Sie verlieren könnten, wenn dies geschieht?

Eine grobe Abschätzung reicht für einen Eindruck von dem Maß an Sicherheit, das für Ihr Unternehmen oder Ihre Institution erforderlich ist. Vermeiden Sie Aufwand für umfangreiche theoretische Modelle, die auf nicht belastbaren Wahrscheinlichkeitsberechnungen basieren.

#2 Pauschale Festlegung zum Schutzbedarf, Mut zur Reduktion

In IT-Sicherheitskonzepten bietet sich der Schutzbedarf von Informationen und Daten als Grundlage zur Festlegung angemessener Maßnahmen an. Diesen Bedarf

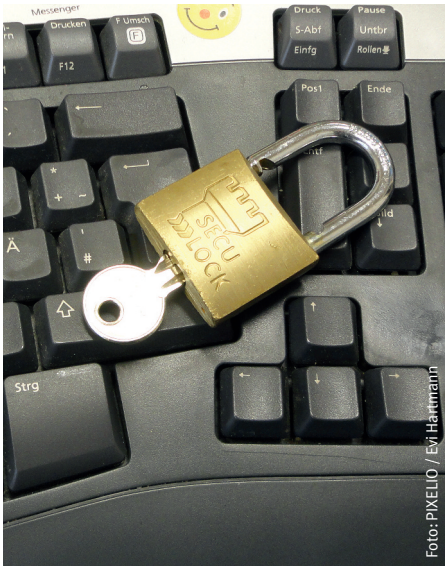

Foto: PIXELIO / Evi Hartmann

festzustellen ist sinnvoll, um ein angemessenes Sicherheitsniveau zu erreichen. Der Aufwand für die Schutzbedarfsfeststellung kann hoch sein, wenn man alle Daten und Anwendungen berücksichtigt. Durch eine pauschale Festlegung des Schutzbedarfs lässt sich dieser Aufwand reduzieren. Beurteilen Sie, ob Sie für Ihre Institution ein allgemeines Ziel-Niveau für IT-Sicherheit oder übergeordnet für Informationssicherheit festlegen können. Benötigen Sie das Sicherheitsniveau von Fort Knox oder verfügen Sie nur über wenige schützenswerte Informationen? Reicht für fast alle verarbeiteten Daten ein „normales“ Schutzniveau aus? Es spart Zeit, wenn man den Schutzbedarf pauschal vorgeben kann. Nur für die Kronjuwelen sollte man auf alle Fälle eine detaillierte Analyse durchführen und identifizieren, an welchen Stellen sie einen höheren Schutzbedarf aufweisen und wie dieser angemessen berücksichtigt werden kann.

Bei einer zu vorsichtigen Bewertung werden Sie viele Anwendungen feststellen, bei denen ein Basis-Schutzniveau vermeintlich nicht ausreicht. Mit Mut zur Festlegung eines normalen Schutzbedarfs und einer bewussten Risikoakzeptanz können Aufwand und Kosten für Sicherheitsmaßnahmen eingegrenzt werden. Bedenken Sie aus Unternehmenssicht, wie hoch IT-basierte Schäden sein können. Nur in Bereichen, die Ihr Unternehmen oder Dritte ernsthaft gefährden, sollte ein Schutzbedarf oberhalb von „normal“ angesetzt werden. Vermeiden Sie Kosten, indem Bereiche „zu gut“ gesichert werden.

#3 Festlegung einer Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten

Ein IT-Sicherheitskonzept stellt die Summe aller als Soll-Zustand festgelegten Maßnahmen zur Reduktion von IT-Sicherheitsrisiken dar. Zwei Möglichkeiten zur Erstellung von Konzepten mit dem Fokus auf Wirtschaftlichkeit sollen vorgestellt werden.

Die Vorgehensweise nach BSI-Standard 100-2 ist bewährt und baut auf den umfassenden IT-Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf. Eine vollständige Umsetzung aller aufgeführten Maßnahmen ist aufgrund des Umfangs und dem Detaillierungsgrad der Kataloge aufwendig. Sofern keine IT-Sicherheitszertifizierung geplant ist kann der Aufwand durch eine Orientie-

rung an diesem Werk reduziert werden. Durch diese abgeschwächte Vorgehensweise, bei denen die Bausteine und Maßnahmen eher als Checkliste verstanden werden und nicht als zwingende Vorgabe, kann mit Augenmaß durchaus auch ein ausreichendes Sicherheitsniveau etabliert werden.

Ein alternativer Ansatz ist die Festlegung und Umsetzung eines institutions-eigenen Basis-Schutzniveaus. Dieses kann beispielsweise durch die Umsetzung der Anforderungen aus den Kontrollzielen im Anhang des Standards ISO 27001 festgelegt werden. Die Kontrollziele decken auf generische Weise alle relevanten Bereiche der Informationssicherheit ab, sind allerdings deutlich abstrakter als die im IT-Grundschutz definierten Anforderungen. Man muss also selbst festlegen, wie das Basis-Schutzniveau konkret aussehen soll und welche Maßnahmen der Basis-Schutz umfasst.

Für „hohen“ oder „sehr hohen“ Schutzbedarf ist in beiden Fällen eine Risikoanalyse und detaillierte Betrachtung von individuellen Gefährdungen und Maßnahmen erforderlich. Berücksichtigen Sie hierbei, gegen welche Art von Angreifern Sie sich schützen wollen. Ein Schutz gegen Fahrlässigkeit und gegen Angreifer, die nicht gezielt gegen Sie agieren, ist bei beiden vorgeschlagenen Vorgehensweisen recht wirtschaftlich möglich. Ein Schutz gegen gezielte Angriffe erfordert hingegen umfangreiche Maßnahmen und ist damit kostenintensiv. Er sollte auf die Kronjuwelen konzentriert werden. Kosteneinsparungen ergeben sich, indem das Erforderliche gemacht wird und nicht das aus Sicherheitssicht Mögliche.

#4 Aufwandsschätzung, Managementunterstützung

Informationssicherheit sollte wirtschaftlich betrieben werden können. Aufwendungen fallen immer an, müssen aber kalkuliert und mit dem Management abgestimmt werden. Teure Maßnahmen sollten langfristig geplant und ggf. auf mehrere Jahre verteilt werden. Die initialen Aufwendungen können durch einen Stufenplan reduziert werden. Nicht von Null auf Hundert ist das Ziel, sondern Fahrt aufzunehmen und diese beizubehalten. Ein Budget sollte sich nicht am Vorjahresbudget orientieren, sondern daran was man in diesem Jahr oder in einem Zweijahres-Zeitraum vorhat.

Der wesentliche Erfolgsfaktor für eine wirksame Informationssicherheit ist neben der Genehmigung der Mittel die Unterstützung durch das Management.

„IT-Sicherheit ist für die Stadt Karlsruhe ein wichtiges Qualitätsmerkmal digitaler Services. Das sieht man auch daran, dass unser Oberbürgermeister Schirmherr der Karlsruhe IT-Sicherheitsinitiative ist.“, so Markus Losert, IT-Leiter der Stadt Karlsruhe. Auch die Erfahrungen des Autors zeigen, dass IT- und Informationssicherheit nur dann gut funktioniert, wenn die Geschäftsführung oder Vorstands-Ebene das Thema wichtig nimmt.

#5 Detailplanung Aufgaben, Nutzung von Werkzeugen

Für die Umsetzung von Konzepten und Maßnahmen sind eine Planung der Aufgaben sowie die Nutzung geeigneter Werkzeuge hilfreich. Werkzeuge können in kleineren Umgebungen Excel-Tabellen oder ein Wiki sein, und auch in größeren Umgebungen kann ein Wiki als Dokumentationswerkzeug sinnvoll sein und um Workflows für Dokumentenlenkung und weitere Aufgabenstellungen erweitert werden. In jedem Fall sollten mühsame manuelle Dokumentationsarbeiten und häufiges Kopieren von Informationen vermieden werden. Legen Sie fest, welche Werkzeuge genutzt werden sollen, welche Informationen an welcher Stelle aufgeführt werden und auch Ihren Anspruch an die Dokumentation. Ein Wiki wird von den Verantwortlichen häufig lieber genutzt als ausgefeilte Vorlagen und Dokumente, die mehr Form als Inhalt aufweisen. Legen Sie eine Qualität für die Inhalte fest und sehen Sie für die Form Freiheitsgrade vor.

Bei der Aufgabenbewältigung kann zudem ein 80:20 Ansatz Aufwand sparen. Etwas noch nicht optimal gemacht zu haben ist im Rahmen eines kontinuierlichen Verbesserungsprozesses (KVP) korrigierbar.

#6 Umsetzen und berichten

Hilfreich für die Umsetzung sind Erfolgserlebnisse und „quick wins“. Maßnahmen, die in der Fläche bei vielen Systemen wirken und sich leicht umsetzen lassen, sollten zeitnah angegangen werden. Versuchen Sie offene Scheunentore zu verschließen anstatt an bereits guten Maßnahmen weiter zu feilen.

Nicht umgesetzte Maßnahmen sollten an das Management gemeldet werden. Hierbei muss nicht jede Detailmaßnahme aufgeführt werden. Wenn es aber Maßnahmen gibt, die wesentliche Störungsauswirkungen vermindern oder Manipulationen erschweren, so sollten diese in Form eines geeigneten Berichts an das Management kommuniziert werden.

#7 Prüfen, Auditieren, Verbessern

Als letzter Schritt wird eine Überprüfung der etablierten Maßnahmen angesetzt. Dies kann in Form einer Eigenüberprüfung erfolgen oder als externer Audit. Definieren Sie eine Vorgehensweise, durch die Verbesserungsmöglichkeiten festgestellt und umgesetzt werden. Informationssicherheit ist ein Prozess und von daher geht es im Anschluss wieder weiter bei Schritt #1.

Es ist besser mit einem einfachen Ansatz anzufangen und diesen kontinuierlich zu verbessern als von Anfang an eine möglichst perfekte Hochsicherheit zu schaffen.

Der Autor: Stefan Gora, Secorvo Security Consultant GmbH, Karlsruhe