Wie sieht meine IT-Strategie aus?

Die vergangenen Wochen haben gezeigt, das Interesse an Daten und Informationen ist ungebrochen hoch. Aber nicht nur staatliche Organisationen möchten an diese gelangen, sondern auch Hacker und Cracker möchten mit diesen Daten Geld verdienen. Daher ist es weiterhin wichtig, seine Informationen zu schützen und nicht den Kopf mit der Begründung «ich kann ja doch nichts machen» hängen zu lassen.

Die IT ist Unterstützer der Business-Prozesse. Auch wenn die IT-Verantwortlichen dies nicht gerne hören, ist die IT-Umgebung «nur» dazu da, das Business optimal zu unterstützen und überhaupt erst zu ermöglichen. Aber um diese Aufgabe erfolgreich zu umzusetzen, muss die IT die Prozesse kennen. Das bedeutet, dass die Geschäftsleitung diese transparent (und in einer für die IT geeigneten Sprache) darstellen muss. Wir empfehlen hier unbedingt eine IT-Strategie, gestützt auf diese Prozesse, zu erstellen. Aus diesem Dokument muss herauskommen, wie kritisch einzelne Prozessschritte sind, welche Verfügbarkeit gefordert, welche Ausfalldauer akzeptiert und welcher maximale Datenverlust verkraftet werden kann. Daraus leitet sich für die IT die technische Umsetzung ab. Unsere Audit-Erfahrungen zeigen, dass hier zu wenig miteinander gesprochen wird und daher einige IT-Projekte nicht zur Zufriedenheit der Geschäftsleitung umgesetzt werden. Mit einer entsprechenden Strategie hätte dies oft verhindert werden können.

Social Engineering

Obwohl in den vergangenen Wochen sehr viel über diese Angriffsart gelesen werden konnte, ist es doch erstaunlich, wie einfach man über diesen Weg an Informationen gelangt. Ein klassisches Beispiel ist der Aufruf an alle Mitarbeiter, an einer Umfrage zum Umgang mit Passwörtern mitzumachen. Wenn das E-Mail noch den Absender des obersten Chefs trägt und ein dicker Preis winkt, ist die Hürde klein, hier mitzumachen. Doch gerade dann ist grosse Vorsicht geboten. Geht der Link wirklich auf das Intranet oder wurde die Umfragewebseite nur gut nachgemacht? Unsere Angriffe, in Absprache mit den verantwortlichen Personen, zeigen eine sehr hohe Erfolgsquote von oft gegen 70 Prozent glaubhafter Antworten.

Doch auch weitere Quellen können für die Informationssuche dienen. Viele Menschen sind sehr unvorsichtig im Umgang mit den eigenen Daten. So können via Xing, Linkedin, Facebook oder der eigenen Webseite bereits sehr viele Informationen zusammengetragen werden. Die Suchmaschine yasni.ch (mit Vorsicht zu benutzen) nimmt dem potenziellen Angreifer die Arbeit ab und durchsucht verschiedene Quellen auf einmal ab und stellt die Informationen übersichtlich dar.

Externe Sicht

Beim Penetration Test geht es darum, einen Weg in die Firma zu finden. Auch hier helfen sogenannte Erfolgsstories von Herstellern, Beschreibungen auf der Firmenwebseite und vor allem Stelleninserate zeigen, was für technische Elemente genutzt werden. Mittels IP- und Portscans können weitere Informationen dazukommen. Vor allem Bannerinformationen sollten, falls immer möglich, verhindert werden. Gibt der Dienst die genaue Version an, kann in Schwachstellendatenbanken nachgesehen werden, ob bereits eine bekannte Angriffsfläche vorhanden ist, die für einen weiteren Schritt genutzt werden kann. Auch gilt es Firewall-, Router- oder gar RDP-Remotezugänge nicht von aussen erreichbar zu konfigurieren. Werden fehlerhafte Loginversuche nicht ausgewertet oder erkannt, kann der Angreifer in Ruhe versuchen, an das richtige Passwort zu gelangen.

Interne Sicht

Kennen Sie die Bilder von Kabeln, die kreuz und quer durch den Serverraum führen? Immer wieder sehen wir dies in unseren Audits. Das macht die Fehlersuche bei Problemen enorm aufwendig. Auch wird der Serverraum gerne als Lagerraum «missbraucht». Dies erhöht die Brandlast und sollte daher immer vermieden werden.

Schwachstellen kommen in jeder Software vor. Früher oder später werden diese entdeckt. Daher ist es enorm wichtig, dass das Patchmanagement sauber und regelmässig durchgeführt wird. Jedoch gilt dies nicht nur für das Betriebssystem, auch die installierten Applikationen benötigen ein Update. Dies ist einer der wichtigsten Aufgaben des Admi-

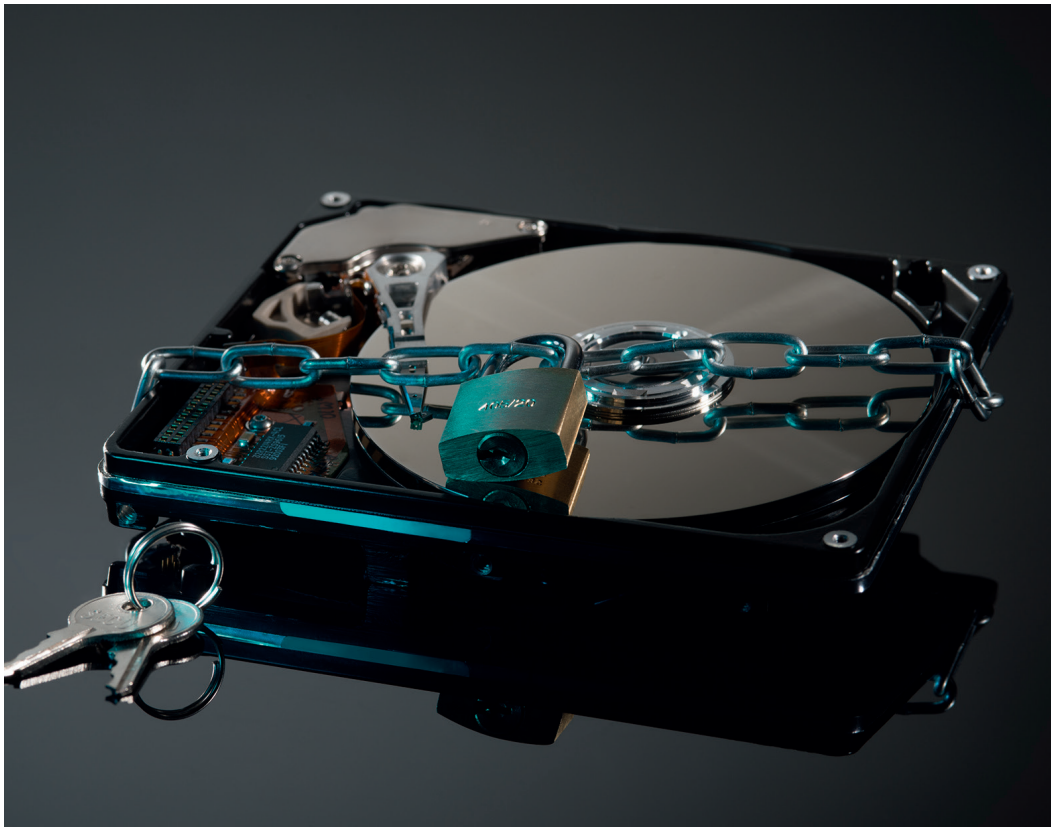

Bild: Archiv

Die Übertragung von Daten wie Passwörter wird zum Glück vermehrt über SSL-geschützte Verbindungen sichergestellt.

nistrators und darf unter keinen Umständen vernachlässigt werden.

Die Übertragung von Daten wie Passwörter wird zum Glück vermehrt über SSL-geschützte Verbindungen sichergestellt (erkennbar am HTTPS). Aus Kostengründen werden aber auch selber erstellte Zertifikate benutzt. Das Problem an diesen Zertifikaten ist die erscheinende Fehlermeldung. Alle aktuellen Browser weisen prägnant auf diesen Missstand hin. Werden die Benutzer geschult diese Fehlermeldung zu ignorieren, wird ein falsches Bild vermittelt. Erscheint diese Fehlermeldung nun beim Aufruf einer Online-Bankingseite, wird gewohnheitsmässig auf «Weiter» geklickt, anstelle die Verbindung sofort abzubrechen. Daher empfehlen wir immer, offizielle Zertifikate anzuwenden, bei welchen keine Fehlermeldung auftritt.

Ein weiteres Problem, welches wir oft feststellen, ist die zu grosszügige Vergabe von Rechten. Werden unter Windows gar die Rechte «Vollzugriff» vergeben, kann der Benutzer selber weiteren Personen Rechte vergeben. Bei den Rechten bleiben bei unvorsichtigen Aufräumvorgängen regelmässig Berechtigungen «liegen», sogenannte SID-Leichen. Ein sauberes Freigabe- und Berechtigungskonzept kann dies verhindern. Bei Stichproben finden wir gelegentlich auch sensible Daten in diesen Verzeichnissen, wie Softwareschlüssel, persönlichen Informationen oder Buchhaltungsdaten. Diese Daten sollten aber unter keinen Umständen in die falschen Hände gelangen.

Cloud-Dienste sind toll, einfach zu installieren und noch einfacher zu nutzen. Doch geschäftliche Informationen gehören hier nicht hin. Hat der Benutzer auf seinem Gerät die notwendigen Rechte weitere Software zu installieren, wird gerne zu Dropbox oder anderen Cloud-Speichern gegriffen. Und schon werden interne Daten zur einfachen Bearbeitung über diese Medien ausgetauscht.

Fazit

Der Administrator hat eine immer wichtigere Aufgabe. Er muss sich um die Angriffsfläche von aussen kümmern und alle Lücken schnellst möglichst schliessen. Aber auch von intern «droht» die Gefahr. Nicht Absicht steht hier an erster Stelle, sondern Unwissenheit, Fahrlässigkeit oder einfach «Faulheit». Daher gilt es, das Angriffspotenzial so klein wie möglich zu halten. Dazu gehört neben einer IT-Strategie, einem IT-Sicherheitskonzept auch ein regelmässiges Patchmanagement. Die Benutzer müssen auf die vorhandenen Gefahren sensibilisiert und Möglichkeiten zum sicheren Umgang mit IT-Mitteln aufgezeigt werden. Auch mit den drohenden Gefahren ist es möglich, die eigene Netzwerkumgebung sicher zu betreiben.

INFOS | KONTAKT

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.gosecurity.ch
info@goout.ch

Anzeige