Empfehlungen

Die sieben wichtigsten Massnahmen, die Sie jetzt treffen können, um Ihr Unternehmen gegen interne Bedrohungen abzusichern

20. Februar 2018, von Irène Wilson

Während von grösseren Hackerangriffen betroffene Unternehmen fast täglich für Schlagzeilen sorgen, sind sich die wenigsten Leute bewusst, dass ein erheblicher Teil dieser Datenschutzverletzungen nicht durch externe Bedrohungen, sondern durch interne Mitarbeitende verursacht werden. Viele Datenschutzverstösse werden von Firmeninsidern begangen, und in der Hälfte dieser Fälle sind die Verstösse nicht auf unglückliche Umstände oder Bedienungsfehler, sondern auf böswillige Handlungen zurückzuführen.

Marktstudien zufolge wenden Schweizer Unternehmen durchschnittlich jeden achten Franken ihrer IT-Budgets für die Sicherheit auf. Der grösste Teil dieser Investitionen fliesst indes in den Schutz des Unternehmens gegen externe Bedrohungen. Aber was ist mit internen Risiken?

Hier sind die sieben wichtigsten Massnahmen, um sicherzustellen, dass Ihr Unternehmen vor

internen Hackerangriffen und Datenschutzverletzungen geschützt ist.

1. Überwachen Sie den «Normalbetrieb» Ihrer IT

Zu diesem Zweck kann ein massgeschneidertes Monitoringsystem implementiert werden, welches sich auf den «Normalbetrieb» Ihres Unternehmens einstellt und Sie informiert, wenn ungewöhnliche Aktivitäten registriert werden. Ein solches System könnte beispielsweise Alarm schlagen, wenn eine Anwendung oder ein Benutzer auf Daten zugreift, für die sie/er keine Zugriffsrechte besitzt. Es könnte Sie auch auf einen verdächtigen Anstieg des Netzwerkverkehrs oder auf Dateitransfers aufmerksam machen, die darauf hindeuten könnten, dass unbefugte Personen Daten aus Ihrem System saugen. Diese Lösungen müssen auf Ihre Organisation zugeschnitten sein. Bei Swiss FTS verfügen wir über ein kompetentes Team, welches ein auf Ihre Bedürfnisse zugeschnittenes Monitoringsystem für Sie implementieren kann.

2. Verschlüsseln Sie die gesamte Datenkommunikation

Mitarbeitende benutzen im Laufe einer Arbeitswoche oft Dutzende von Anwendungen, die eine Anmeldung und eine Authentifizierung erfordern. Wenn die Verbindungen zu diesen Diensten nicht verschlüsselt sind, kann jedermann im Netzwerk auf die Zugangsdaten der anderen Anwender zugreifen. (Falls die Anwendungen extern gehostet werden, können sich sogar Personen ausserhalb des Unternehmens Zugang zu den Logindaten verschaffen.) Aus diesem Grund sollte die gesamte Kommunikation mit Anwendungen und Diensten stets in verschlüsselter Form erfolgen, sei es mit Hilfe von SSL oder mit einer anderen Verschlüsselungstechnologie. Darüber hinaus kann die Single-Sign-on (SSO) Technologie Ihrem IT-Team helfen, sicherzustellen, dass alle Mitarbeitenden sichere Zugangsdaten verwenden. SSO kann die Benutzung sicherer Kanäle so weit vereinfachen, dass Ihre Mitarbeitenden gar nicht mehr merken, dass sie diese benutzen.

3. Stärken Sie das Sicherheitsbewusstsein der Mitarbeitenden durch entsprechende Trainings

Die Mitarbeitenden sollten dafür geschult werden, die wichtigsten Arten von externen und internen Angriffen und Bedrohungen zu erkennen. So sollten Mitarbeitende beispielsweise darauf trainiert werden, niemals Programme aus unbekannten oder verdächtigen Quellen auszuführen. Ebenso sollten sie in der Lage sein, Phishing und andere bösartige Angriffe zu

erkennen. Sie sollten lernen, niemals USB-Laufwerke oder andere Geräte anzuschliessen, die sie irgendwo gefunden oder aus unbekannten Quellen zugespielt erhalten haben; solche USB-Laufwerke sollten entweder direkt entsorgt oder zur Überprüfung in einer sicheren Umgebung an IT übergeben werden. Des Weiteren muss das Bewusstsein der Mitarbeitenden für Social Engineering geschärft werden, damit sie keine vertraulichen Informationen an unbekannte Personen weitergeben, die sich beispielsweise als Leiter einer anderen Geschäftsstelle ausgeben. Es ist wichtig, dass Ihren Mitarbeitenden qualitativ hochstehende Schulungen zu diesen Themen angeboten werden.

4. Sorgen Sie dafür, dass jeder Mitarbeitende nur auf jene Daten zugreifen kann, die er tatsächlich benötigt

Die Implementierung eines Zugriffskontrollsystems kann das Risiko von internen Datenschutzverletzungen drastisch reduzieren, da jeder Mitarbeitende nur auf einen Bruchteil der Unternehmensdaten bedarfsorientiert zugreifen kann.

5. Das Vier-Augen-Prinzip

Für Änderungen an den System- und Sicherheitseinstellungen und die Gewährung von Zugriffsrechten sollte Ihr Unternehmen das «Vier-Augen-Prinzip» befolgen – dies bedeutet, dass alle Änderungen an diesen systemweiten Einstellungen stets von mindestens zwei Personen vorgenommen bzw. überwacht werden. Die Auswahl eines falschen Kontrollkästchens oder die Verschiebung der Sicherheitsrichtlinien an einen falschen Ort kann gravierende Folgen haben. Stellen Sie sich vor, was passieren könnte, wenn ein Temporärmitarbeiter versehentlich Administratorrechte für eine ganze Domain erhielte. Solche potenziell katastrophalen Sicherheitspannen lassen sich minimieren, wenn an allen wichtigen Änderungen der Systemeinstellungen zwei Personen beteiligt sind.

6. Aufteilung der Zuständigkeiten

Es ist insbesondere in kleineren Unternehmen erstaunlich verbreitet, dass ein Administrator die volle Kontrolle über die gesamte IT hat. Dies ist eine gefährliche Situation, da diese Person Ihr gesamtes Unternehmen lahmlegen könnte. Wir empfehlen Ihnen, Ihre geschäftskritischen Systeme zu trennen und die Verantwortung für deren Administration auf verschiedene Personen zu übertragen. Dies wird Ihre IT-Infrastruktur erheblich sicherer und

robuster machen.

7. Bringen Sie das gesamte Unternehmen an einen Tisch

Das Thema Sicherheit beschränkt sich nicht allein auf die IT. Es betrifft das gesamte Unternehmen. Dazu zählen das Management ebenso wie HR, der Verkauf, die Rechtsabteilung usw. Es ist wichtig, dass alle Anspruchsgruppen dies verstehen und gemeinsam auf das Ziel einer höheren unternehmensweiten Sicherheit hinarbeiten. Schliesslich macht es wenig Sinn, umfangreiche Mittel in eine ausgeklügelte Sicherheitsinfrastruktur zu investieren, wenn diese von den Mitarbeitenden nicht akzeptiert oder nicht vorschriftsgemäss genutzt wird. Wir empfehlen Ihnen, sich nicht nur auf den Aspekt der IT-Sicherheit zu fokussieren, sondern darüber hinaus auch eine unternehmensweite Kultur anzustreben, welche die Sicherheitsthematik ernst nimmt und jederzeit adäquate Sicherheitsmassnahmen umsetzt.

Bei unserer Arbeit im Bereich der IT-Forensik stellen wir immer wieder fest, dass die oben beschriebenen Massnahmen nicht korrekt umgesetzt werden. Dies kann zu sicherheitsrelevanten Vorfällen führen, die gravierende Auswirkungen auf Ihren Geschäftsbetrieb haben können. Wir möchten gerne die Erfahrungen mit Ihnen teilen, die wir bei der Einrichtung eines Information Security Management Systems (ISO 27001-Zertifizierung) innerhalb von Unternehmen gesammelt haben.

Irène Wilson

Irene Wilson ist auf digitale Forensik und eDiscovery spezialisiert und hat im Laufe ihrer langjährigen Erfahrung für Kunden aus einer Vielzahl von Branchen in ganz Europa gearbeitet. Zu ihren Qualifikationen gehören die renommierten Master-Titel für Nuix Workstation und Nuix Discover.

Swiss FTS AG | www.swiss-fts.com | +41 43 266 78 50 | info@swiss-fts.com