So nah.
So gut.

Gehrke Econ

ge Information

IT-Sicherheit ist Chefsache

Ergebnisse unserer IT-Audits

Inhalt

Gehrke Econ ist als Wirtschaftsprüfungsunternehmen unter anderem dazu verpflichtet, im Rahmen von Jahresabschlussprüfungen bei unseren Mandanten, mittels der Durchführung von IT-Audits, die Sicherheit rechnungslegungsrelevanter IT-Systeme zu beurteilen. Diese IT-Audits haben uns in den letzten Jahren einen tiefen Einblick in den Aufbau, die Organisation und die Wirkungsweise der jeweiligen IT-Systeme gegeben und auch die Akzeptanz in der Geschäftsführung deutlich gemacht. Diese Einblicke und Ergebnisse möchten wir in diesem Rundschreiben exklusiv mit Ihnen teilen.

Grundsätzlich ließ sich feststellen, dass sich das Commitment und Bewusstsein für die Relevanz sowie Notwendigkeit von IT-Sicherheit bei den Führungskräften erhöht hat. Dennoch zeigen die Ergebnisse unserer IT-Audits, dass eine Vielzahl von Unternehmen noch nicht die zur Verfügung stehenden technischen und organisatorischen Möglichkeiten in ausreichendem Maße nutzen.

Schwachstellen in der IT-Sicherheit können zum Verlust der Verfügbarkeit und Integrität der IT-Systeme und Firmendaten führen. Störungen der Wertschöpfungsprozesse bis zur Handlungsfähigkeit, Bußgelder auf Grund von Datenschutzverletzungen, ein Reputationsverlust bei Shareholdern sowie die Wiederherstellung der IT-Systeme sind weitere mögliche unerwünschte Folgen. Es entstehen unnötige Kosten, die erfahrungsgemäß bis in die Insolvenz führen können.

IT-Audit

- Das IT-Audit im Rahmen einer Jahresabschlussprüfung gilt der Feststellung, ob risikobehaftete IT-Bereiche anhand vorhandener Kontrollmechanismen ausreichend adressiert werden und damit die Verfügbarkeit, Vertraulichkeit sowie Integrität rechnungslegungsrelevanter IT-Systeme einschließlich der verarbeiteten Finanzdaten sichergestellt ist.

- Ein IT-Audit erstreckt sich dabei auch auf die Aufnahme und Beurteilung des IT-Systemumfelds, die Prüfung der IT-Organisation, umgesetzte Maßnahmen der Cyber- und Informationssicherheit sowie die Notfallvorsorge.

IT-Compliance & Assurance

- Wirtschaftsprüfungsunternehmen sind gesetzlich verpflichtet, regelmäßig IT-Audits bei ihren Mandanten durchzuführen. Aufgrund der digitalen Transformation und der sich fortlaufend erhöhenden Komplexität der IT-Systeme wurden die IT-Prüfvorgaben durch den Gesetzgeber erneut erweitert und verschärft.

- Als Maßstab für die Beurteilung der IT-Systeme werden durch die Wirtschaftsprüfer dabei neben den gesetzlichen Bestimmungen diverse Rechnungslegungsvorschriften, Stellungnahmen und Erlasse herangezogen.

Ergebnisse unserer IT-Audits

- Die Ergebnisse unserer IT-Audits basieren auf den Prüfungen von kleinen und mittelständischen Unternehmen (KMU) aus verschiedenen Branchen. Sie stellen keine repräsentative Statistik dar. Dennoch sind alle Erkenntnisse zu würdigen, da in überdurchschnittlich vielen Unternehmen umfangreiche und kritische Mängel in der IT-Sicherheit identifiziert wurden.

- Die Ziele der IT sind nicht immer definiert und können dadurch von den Unternehmenszielen abweichen. Die IT Abteilung ist ohne direkte Anbindung an die Geschäftsführung und entwickelt sich in eine andere Richtung als das Unternehmen.

- Die personellen Ressourcen der IT-Abteilung sind selten ausreichend, um den Anforderungen des Unternehmens gerecht zu werden. Es besteht oft eine Abhängigkeit von einzelnen Wissensträgern.

- Mitarbeiter der IT-Abteilung verfügen nicht immer über das notwendige Fachwissen, wodurch die Anforderungen an die IT-Sicherheit nicht angemessen umgesetzt werden können.

- Nicht alle Mitarbeiter sind in der Lage, sicher mit ihren IT-Ressourcen umzugehen (im Büro und zuhause). Selten sind sie ausreichend für Cyber-Risiken, wie z.B. Social Engineering, sensibilisiert und im Umgang mit Notsituationen geschult.

- Wenige Unternehmen haben ihre kritischen Wertschöpfungsprozesse und IT-Systeme eindeutig identifiziert, wodurch keine Ableitung von IT-Sicherheitsmaßnahmen gemäß der Daten- und Systemkritikalität erfolgen kann.

- Ein vollumfängliches IT-Asset-Management ist selten vorhanden. Die vorhandene Hard- und Software ist nicht vollständig inventarisiert. Es mangelt an Klarheit über den tatsächlichen Bestand, wodurch notwendige Schutzmaßnahmen nicht flächendeckend umgesetzt werden.

- Oft sind Verfahren zum IT-Risikomanagement nicht oder nicht ausreichend etabliert, wodurch Risiken aus der IT nicht erkannt werden. Eine Ableitung und Umsetzung von angemessenen Schutzmaßnahmen kann nicht erfolgen. Ein dediziertes IT-Sicherheitskonzept ist selten vorhanden.

- Die Wiederaufnahme der Geschäftstätigkeit ist nach einem IT-Ausfall nicht oder nicht in angemessener Zeit möglich. Oft fehlt ein anwendbares Notfallkonzept sowie Übung im Umgang mit Notfallsituationen.

- Die Sicherheitseinrichtungen von Supply-Chain-Partnern und Kunden werden unzureichend betrachtet. Schwachstellen im Sicherheitssystem der Dienstleister könnten zu einer unzureichenden Leistungserbringung und damit zu einer Störung wesentlicher Geschäftsprozesse führen.

- Unzureichende physische Sicherungsmaßnahmen der Serverräume und Rechenzentren gefährden den ordnungsgemäßen Betrieb. Zutrittsberechtigungen zu Technikräumen sind selten formuliert und Zutritte nicht nachvollziehbar protokolliert.

- Es existieren Sicherheitslücken durch veraltete Betriebssysteme sowie Datenbanken, da Software- und Sicherheitsupdates nicht zeitgerecht durchgeführt werden.

- In wenigen Fällen gibt es einen unzureichenden Virenschutz, der zum Verlust der Verfügbarkeit und Integrität relevanter Informationen führen kann.

- Technische Sicherungsmaßnahmen für den Zugriff auf die IT-Systeme von intern, und das Unternehmensnetzwerk von extern, sind selten angemessen. Es kommt zum unautorisierten Zugriff auf Systeme und Daten.

- Es fehlen Rollen- und Rechtekonzepte, um fachlich angemessene Definitionen mit technischen Rollen und restriktiven Rechten in den IT-Systemen zu verknüpfen. User- und Rechtereviews werden nicht regelmäßig durchgeführt. Die Datenintegrität ist aufgrund von unautorisiertem Zugriff gefährdet. Unberechtigte Personen erhalten Zugriff auf sensible Unternehmensdaten.

- Vorgaben und Kontrollen für Änderungen an den IT-Systemen sind nicht formuliert. Dadurch gelangen Änderungen in die IT-Systeme und verhindern, dass Daten richtig, vollständig und korrekt verarbeitet werden können.

- Datensicherungen erfolgen nicht regelmäßig und werden nicht auf Vollständigkeit überprüft. Wiederherstellungstests aus dem Backup werden nicht durchgeführt. Es besteht das Risiko eines Datenverlustes.

- Ein Monitoring der Hardwarekomponenten erfolgt nicht oder unvollständig. Dadurch kommt es zum Hardwareausfall, was u.a. zum Verlust der Verfügbarkeit der IT-Systeme und Daten führt.

- Die gesetzlich vorgeschriebenen Verfahrensdokumentationen rechnungslegungsrelevanter Prozesse und IT-Systeme sind kaum vorhanden bzw. unvollständig oder nicht aktuell. Ohne Dokumentation über die angemessene Umsetzung und Einhaltung der GoBD-Anforderungen können Nachweis- und Rechenschaftspflichten nicht erfüllt werden.

Ursachen & Gründe

- Viele Unternehmen besitzen kaum Kenntnisse über das eigene Risikoprofil und die allgemeine Cyber-Bedrohungslage, wodurch ein Bewusstsein für notwendige Investitionen in IT-Sicherheit fehlt.

- Einigen Geschäftsführern ist nicht bewusst, welche finanziellen Auswirkungen eine mangelhafte IT-Security auf die Performance des Unternehmens haben wird. Der Human-Factor wird als IT-Sicherheitsrisiko unterschätzt.

- Unternehmen, die sich bereits über die Risiken aus dem Gebrauch von IT-Systemen bewusst sind, fehlt es an Fachpersonal mit notwendigem Know-How und zeitlichen Ressourcen. Oft mangelt es an ausreichendem Budget, um sich als potenzieller Arbeitgeber gegen Mitbewerber zu behaupten.

- Auch bei der Nutzung externer IT-Dienstleister vertrauen Unternehmen darauf, dass „alles“ sicher ist, überprüfen dieses jedoch nicht. Es fehlen angemessene Kontrollmaßnahmen.

Empfehlungen

- Beantworten Sie für sich die Frage, wie lange Sie ohne Ihre IT-Systeme sowie Daten handlungsfähig sind und Ihre Wertschöpfungsprozesse aufrechterhalten können. Stellen Sie fest, ob Ihr Unternehmen wirksam gegen Cyber-Risiken geschützt ist.

- Erstellen Sie einen Notfallplan, um die Funktion der kritischen IT-Systeme und Daten in angemessener Zeit wiederherzustellen. Simulieren Sie den Ernstfall. Schulen und sensibilisieren Sie alle Mitarbeiter für IT-Sicherheit.

- Legen Sie Informationssicherheitsziele fest. Führen Sie eine Risikoanalyse durch und setzen Sie ein IT-Sicherheitskonzept mit wirksamen organisatorischen und technischen Maßnahmen um.

- Vervollständigen und aktualisieren Sie die Dokumentation der IT-Systemlandschaft. Richten Sie ein internes Kontrollsystem ein. Verifizieren Sie regelmäßig die Wirksamkeit Ihrer Sicherheitseinrichtungen und schließen Sie sukzessive alle Schwachstellen nachhaltig.

- Übernehmen Sie proaktiv Engagement und Verantwortung für IT-Sicherheit. Nehmen Sie notwendige IT-Sicherheitsmaßnahmen in die strategische Planung auf, stellen Sie benötigte Ressourcen bereit und benennen Sie Sicherheitsverantwortliche.

- Erstellen bzw. aktualisieren Sie die gesetzlich vorgeschriebenen Verfahrensdokumentationen über Ihre rechnungslegungsrelevanten Prozesse und IT-Systeme.

- Verzichten Sie auf unnötige Kosten durch vermeidbare Störungen und Wiederherstellung Ihrer IT-Systeme sowie Wertschöpfungsprozesse, Bußgelder durch Datenschutzverletzungen und einen Reputationsverlust bei Ihren Shareholdern.

Wir unterstützen Sie!

Falls Sie sich in Themen der IT-Compliance und Assurance unsicher sind, kommen Sie gerne auf uns zu. Für eine persönliche Beratung stehen die Ihnen bekannten Kolleginnen und Kollegen von Gehrke Econ sowie Norman Escherich (norman.escherich@gehrke-econ.de) zur Verfügung.

IT-Sicherheit ist Chefsache - Sprechen Sie uns an, wir beraten Sie gerne!