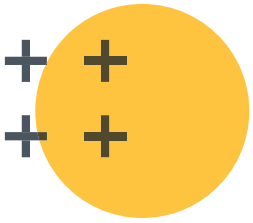
Cybersicherheit: Erfolgreiche Strategien in der WP-Praxis

Von Stefan Schmittner und Andreas Schneider



Neben großen Konzernen geraten immer mehr mittelständische Unternehmen ins Visier der Cyberkriminellen. Auch Wirtschaftsprüfungsgesellschaften bleiben davon nicht verschont. Stefan Schmittner und Andreas Schneider von GKK Partners über aktuelle Trends und erfolgreiche Strategien gegen die Cyberangriffe.

Die größte Gefahr für die IT-Sicherheit in Deutschland geht derzeit vor allem von den Angriffen mit Ransomware und von den sogenannten Distributed-Denial-of-Service-Attacken (DDoS-Attacken) aus. Das belegt der aktuelle Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Mit Hilfe von Ransomware-Angriffen verschaffen sich Cyberkriminelle Zugriff auf IT-Systeme. Dabei werden sie gezielt mit einer Schadsoftware verschlüsselt. Die Produktivsysteme sind anschließend nicht mehr nutzbar. Für die Entschlüsselung und Wiederherstellung verlangen die Angreifer eine Lösegeldzahlung. Um den Druck auf das betroffene Unternehmen zu erhöhen, drohen sie zudem oft damit, sensible Daten und Informationswerte zu veröffentlichen. Bei den DDoS-Attacken wird das Zielsystem mit Anfragen überhäuft, um den Service stark einzuschränken beziehungsweise lahmzulegen. Diese Art des Angriffs wird vor allem bei Webseiten oder Online-Services angewendet.

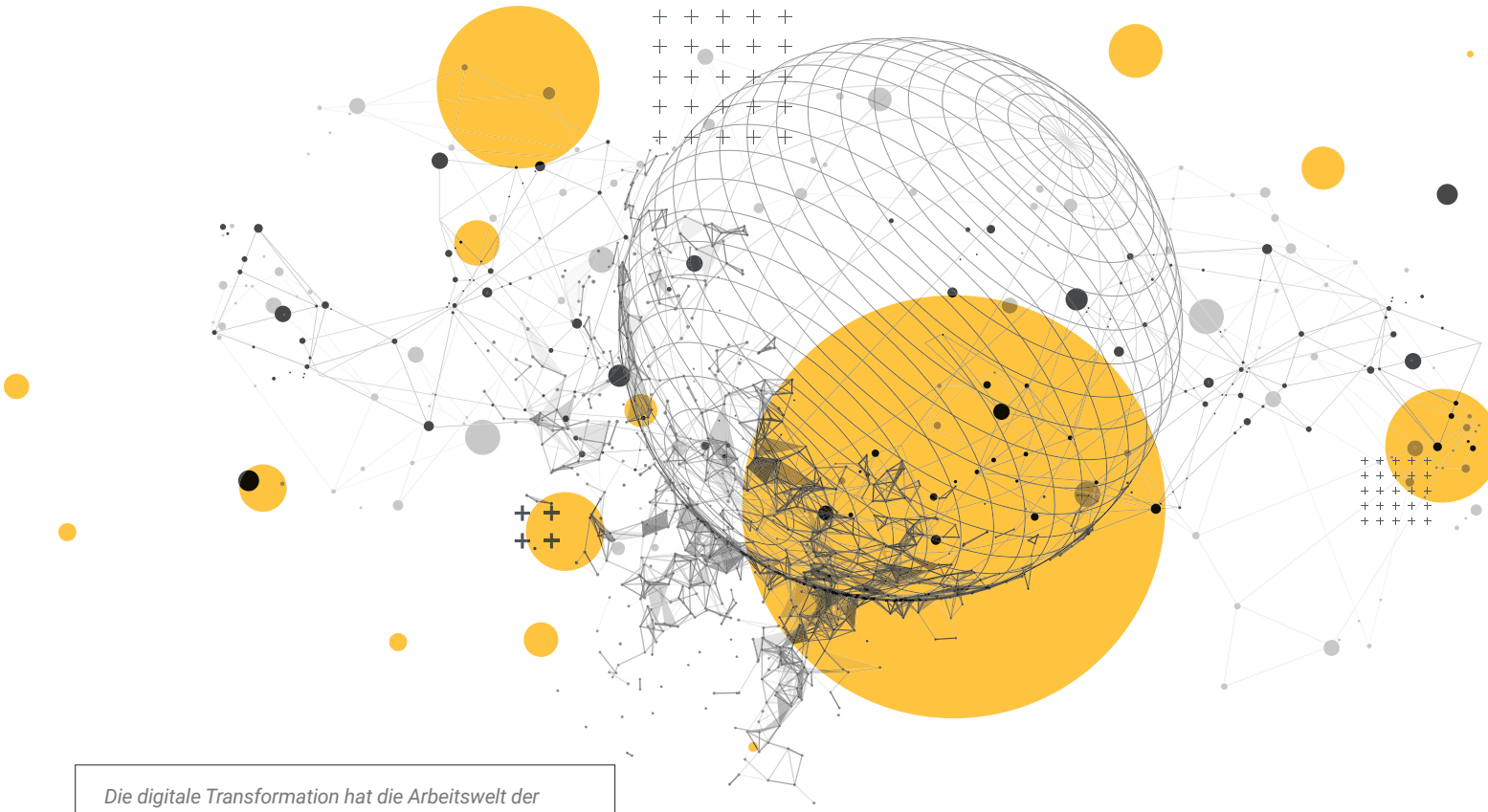
Cybersicherheit als Teil der Strategie

In der Praxis reicht oft schon eine versehentlich angeklickte Phishing-Mail aus, um Cyberkriminellen ein Einfallstor in das Unternehmensnetzwerk zu öffnen. Um diesen Risiken zu begegnen und mandantenspezifische Informationswerte in Wirtschaftsprüfungsgesellschaften zu schützen, müssen technische und organisatorische Maßnahmen zur IT-Sicherheit festgelegt und implementiert werden.

Es ist davon auszugehen, dass die Professionalität der Angreifer sich künftig verstärken wird. Cybersicherheit muss daher bereits heute ein integraler Bestandteil der strategischen Weiterentwicklung von jedem Unternehmen sein. Wirtschaftsprüfer sollten vor allem im Hinblick auf die Sensibilität der ihnen anvertrauten Daten und Informationen dabei eine Vorreiterrolle einnehmen. Ein erfolgreicher Cyberangriff kann bei einer Wirtschaftsprüfungsgesellschaft nicht zuletzt zu einem erheblichen Reputationsschaden führen.

Maßnahmen für höhere Cybersicherheit

Mandantenbezogene Unterlagen und Dokumentationen werden heute überwiegend elektronisch verarbeitet. Das spart Zeit und ermöglicht flexiblere Arbeitsmodelle. Gleichzeitig bringt das



Die digitale Transformation hat die Arbeitswelt der Wirtschaftsprüfer verändert und ihnen ein flexibles, effizientes und vernetztes Arbeiten ermöglicht. Gleichzeitig geht damit jedoch auch ein erhöhtes Risiko von Cyberkriminalität einher und erfordert gute Strategien.

auch Risiken mit sich, wenn zum Beispiel sensible Daten über nicht angemessen gesicherte Übertragungswege aus dem Homeoffice ausgetauscht werden. An dieser Stelle ist nicht nur die Implementierung von technischen Maßnahmen, etwa in Form von Zugangs- und Zugriffskontrollen oder verschlüsselten Datenübertragungen relevant, sondern auch ein angemessenes Verständnis von Cybersicherheit bei allen Beteiligten erforderlich.

Gängige IT-Frameworks und Normen, wie COBIT, ISO 27001 und IT-Grundschutz-Kompendium des BSI, beinhalten eine Vielzahl von Maßnahmen, mit denen Wirtschaftsprüfungsgesellschaften die Cybersicherheit erhöhen können:

Inventarisierung von IT-Komponenten
Um IT-Systeme und IT-Anwendungen angemessen zu schützen, empfiehlt sich eine Inventarisierung aller eingesetzten IT-Komponenten. Sie hilft dabei, potenzielle Angriffsziele zu identifizieren und den Überblick über die eingesetzten IT-Komponenten zu behalten. Zudem eignet sich die Inventarisierung als Ausgangsbasis für ein Informationssicherheitsmanagementsystems (ISMS).

Festlegung von Zugangs- und Zugriffskontrollen
Für jedes eingesetzte IT-System ist ein Benutzerberechtigungskonzept mit klar definierten Rollen und Verantwortlichkeiten unerlässlich. Besonders die Zuweisung der erforderlichen Berechtigungen sollte an die individuellen Bedürfnisse des Unternehmens ausgerichtet und dokumentiert werden.

Für jeden Mitarbeiter der Wirtschaftsprüfungsgesellschaft ist ein personenbezogener Account erforderlich. Wichtig dabei: das Prinzip der minimalen Berechtigungsvergabe und das Prinzip der Funktionstrennung.

Ratsam ist ein Freigabeprozess, der den Zugang neuer Benutzer steuert und die beiden Prinzipien berücksichtigt. Anträge sollten nur durch autorisiertes Personal im Mehraugenprinzip freigegeben und zur besseren Nachvollziehbarkeit zentral verwaltet werden.

Es ist sinnvoll, die Mindestvorgaben zur Ausgestaltung von Passwörtern für die IT-Systeme auf Applikations-, Datenbank- und Betriebssystemebene direkt systemseitig zu hinterlegen und in einer IT-Sicherheitsrichtlinie zu definieren. Die

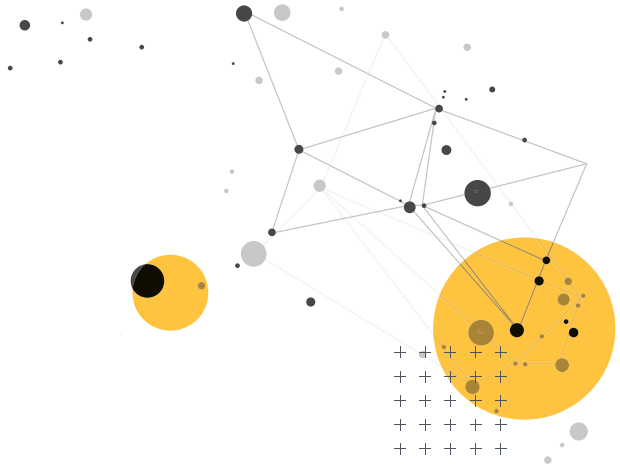
CYBERSICHERHEIT

Eine absolute Cybersicherheit ist kaum zu erreichen — weder heute noch in der Zukuft. Mit richtigen Strategien und geeigneten Maßnahmen lassen sich die Risiken der Cyberangriffe allerdings stark reduzieren und ein hohes Cybersicherheitsniveau aufbauen.

Best-Practice-Ansätze des BSI bieten hier eine gute Orientierung. Neben dem klassischen Login mit Benutzer und Passwort empfiehlt sich zudem eine mehrstufige Authentifizierungsmethode.

Datensicherung und Wiederherstellung

Vor allem bei einem Ransomware-Angriff ist ein angemessenes Datensicherungs- und Wiederanlaufverfahren ein entscheidender Erfolgsfaktor. Ein klar definiertes Datensicherungskonzept ist hier unverzichtbar. Es beschreibt die IT-Systeme der WP-Kanzlei, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen.
Es muss festgelegt werden, wie hoch der maximale Datenverlust (Recovery Point Objective) und die maximale Wiederherstellungszeit (Recovery Time Objective) sein dürfen. Besonders bei Auslagerungsverhältnissen sollten diese Zeiten mit dem externen IT-Dienstleister schriftlich vereinbart werden. Darüber hinaus sind eindeutige Verantwortlichkeiten innerhalb der Wirtschaftsprüfungsgesellschaft zu definieren.



Update- und Patchmanagement

Angreifer nutzen verstärkt den Zugang über Software-Komponenten mit veralteten Patch- und Versionsständen, beispielsweise von Betriebssystemen und Anwendungssoftware. Deshalb sind regelmäßige Updates ein Muss. Nicht oder zu spät installierte Updates können fatal sein.

Firewall und Virenschutz-Software

Eine für die jeweilige Größe der Prüfungsgesellschaft angemessene Firewall und Virenschutz-Software sorgen dafür, dass potenzielle Schadsoftware bereits im Vorfeld blockiert werden. Anomalien im Netzwerk können so frühzeitig identifiziert werden.

HINWEIS: SOLON X

Zum Thema Cyber Security im Mittelstand lesen Sie bitte auch den Beitrag "Cybersicherheit geht uns alle an" von Tobias Diemer (Transferstelle Cybersicherheit im Mittelstand) auf www.solon-x.de.

IT-Outsourcing
Zunehmend setzt sich der Trend zu einer Cloud-First-Strategie auch bei Wirtschaftsprüfungsgesellschaften durch. Cloud-Lösungen können von Vorteil sein, weil sie den aktuellen Sicherheitsstandards entsprechen und skalierbar sind. Allerdings ist die WP-Kanzlei auch bei einer Auslagerung weiterhin für die gespeicherten Daten verantwortlich. Deshalb sollte bei der Wahl des IT-Dienstleisters auf die Bescheinigungen wie BSI C5 (Cloud Computing Compliance Criteria Catalogue) oder ISAE 3402 Typ II geachtet werden. Das gilt auch für Portale, die für den Austausch von Dokumentationen und Unterlagen zwischen der Prüfungsgesellschaft und den Mandanten eingesetzt werden.

Awareness-Maßnahmen
Neben den rein technischen Maßnahmen ist es von entscheidender Bedeutung, Mitarbeiter für das Thema Cybersicherheit zu sensibilisieren. Regelmäßige Awareness-Trainings, etwa durch die Simulation von Phishing-Angriffen, schärft die Wahrnehmung für potenzielle Spam-Mails mit Schadcode. In der Praxis sind die Sensibilisierung und kritische Grundhaltung eines jeden Mitarbeiters von entscheidender Bedeutung für die Wirksamkeit der eingerichteten Sicherheitsmaßnahmen.

Fazit
Eine vollumfängliche Sicherheit ist auch künftig nicht zu erreichen. Mit technischen und organisatorischen Maßnahmen können sich Wirtschaftsprüfungsgesellschaften jedoch vor möglichen Cyberangriffen schützen. Ein hohes Cybersicherheitsniveau stärkt das Vertrauen der Mandanten in den Wirtschaftsprüfer. Mehr noch: Angesichts der Sensibilität der vorgehaltenen Daten sollten Wirtschaftsprüfer eine Vorreiterrolle in Sachen Cybersicherheit einnehmen und entsprechende Sicherheitsmaßnahmen bei der strategischen Ausrichtung der Kanzlei angemessen berücksichtigen.

Stefan Schmittner ist Wirtschaftsprüfer, Steuerberater, CISA, CVA und arbeitet bei GKK Partners an der Schnittstelle zwischen Informationstechnologie, Wirtschaftsprüfung und Steuerberatung. Dort betreut er vor allem mittelständische Unternehmen. Er verfolgt einen ganzheitlichen Beratungsansatz und entwickelt dabei für seine Mandanten passgenaue Lösungen bei digitalen Projekten.

Stefan Schmittner

Andreas Schneider

Andreas Schneider ist CISA, Prüfer für interne Revisionssysteme (DIIR), Lead Auditor ISO 27001 und arbeitet bei GKK Partners im Bereich IT Consulting. Dort betreut er insbesondere mittelständische Unternehmen bei der digitalen Transformation. Als CISA und Lead Auditor ISO 27001 entwickelt er maßgeschneiderte Lösungen für seine Mandanten, um die Cyberresilienz zu erhöhen.