ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 04 | Dezember 2011 | www.isaca.ch
NEWSLETTER

Social Engineering
Die Angriffsform nutzt die Schwachstelle Mensch aus und erfordert anspruchsvolle Schutzmassnahmen **Seite 75**

CISA
Für das älteste der vier ISACA-Personenzertifikate muss eine vierstündigen Prüfung bestanden werden **Seite 79**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 79**

Social Engineering – Theorie und Praxis

«Guten Tag Frau Müller, hier ist Herr Meier von der IT. Wir haben gerade ein grosses Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet Ihr Passwort?» Ein plumper, aber umso erfolgreicherer Trick, wenn es darum geht an vertrauliche Informationen mittels Social Engineering zu gelangen.

Von Reto C. Zbinden

Um ein Unternehmen über das Internet oder direkt anzugreifen und so vertrauliche Informationen zu erlangen, nutzen Social Engineers die Gutgläubigkeit, Bequemlichkeit, Höflichkeit oder sogar die Begeisterungsfähigkeit der Menschen aus. Aus diesem Grund ist es anspruchsvoll, gegen einen Angriff Schutzmassnahmen zu ergreifen, denn die Opfer merken oft gar nicht, dass sie hintergangen wurden oder sie weigern sich dies überhaupt zuzugeben. Die Motive eines Social Engineers, also einer Person, die versucht unbefugterweise Zugriff auf Computersysteme, Informationen oder andere Objekte zu erlangen, ähneln denen eines Hackers: Sie wollen an Geldmittel, Informationen oder IT-Ressourcen eines Unternehmens gelangen.

Ein Social Engineer versucht Mitarbeitende zur Preisgabe von Informationen zu überreden, die es ihm erlauben, ohne angemessene Autorisierung IT-Systeme oder Systemressourcen zu nutzen oder sich entsprechend unbefugt Informationen zu beschaffen. Ein solches Vorgehen wird üblicherweise als Trickbetrug bezeichnet.

Art. 146 StGB Absatz 1 hierzu lautet wie folgt: «Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen andern am Vermögen schädigt…». Geschieht der Social Engineering-Angriff jedoch bezüglich einer Datenverarbeitungsanlage, kommt Art. 147 StGB Absatz 1 zum Tragen: «Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt…». Beide Artikel sehen eine Geldstrafe oder eine Freiheitsstrafe von bis zu fünf Jahren vor.

Viele Unternehmen sind ungeachtet ihrer Grösse der Ansicht, dass Social Engineering-Angriffe nur ein Problem für die «Anderen» darstellt, da sich ein Angriff nur dort lohnen würde. Dies mag in der Vergangenheit so gewesen sein. Der Anstieg der Internetkriminalität zeigt jedoch, dass es Angreifer nun auf alle Nutzer von Informatik- und Kommunikationstechnologien abgesehen haben, vom Grosskonzern bis zum Einzelbenutzer. Viele Kriminelle bestehlen Unternehmen direkt, indem

sie Finanzmittel und Ressourcen umleiten. Andere verwenden jedoch auch Unternehmen als Mittel zum Zweck für kriminelle Aktionen gegen andere. Auf diese Weise sind sie entsprechend auch für Behörden wesentlich schwerer zu fassen.

Um Mitarbeitende und Unternehmen vor Social Engineering-Angriffen zu schützen, muss man die Angriffsformen und -motive kennen und sich bewusst sein, was Angreifer im eigenen Unternehmen suchen könnten und abschätzen, welche Verluste dies für das Unternehmen bedeuten könnte. Mit diesem Wissen können vorhandene interne Regelungen um präventive Massnahmen und Regeln gegen Social Engineering-Angriffe ergänzt werden. Diese Massnahmen und die notwendigen flankierenden Ausbildungs- und Sensibilisierungsmassnahmen sollen dem Mitarbeitenden helfen, im Fall der Fälle richtig zu reagieren.

Die Angriffsvektoren

Im Allgemeinen versuchen Social Engineers, ihre Angriffe, abhängig von Motiv und Gelegenheit, über alle Kanäle auszuführen, die aus und in das Unternehmen führen, dazu gehören typischerweise:

- Online via E-Mails
- Telefon
- Abfallentsorgung
- Persönliche Kontakte
- Reverse Social Engineering

Es reicht jedoch nicht aus, nur diese Angriffspunkte zu (er)kennen, man muss sich auch entsprechend bewusst sein, auf was es die Angreifer abgesehen haben könnten. Deren Motive beruhen auf dem Streben nach Dingen, die uns alle antreiben: Geld, sozialer Aufstieg oder Selbstwertgefühl. Sie wollen Geld oder Ressourcen, sie wollen Anerkennung in der Gesellschaft oder unter ihresgleichen, und sie möchten stolz auf sich selbst sein. So versuchen Social Engineers, diese Ziele illegal durch Diebstahl oder Eindringen in Systeme zu erreichen. Angriffe jeder Art sind für ein Unternehmen kostspielig, sei es wegen entgangener Umsätze, entwendeter Ressourcen, veruntreuter Informationen, eingeschränkter Verfügbarkeit oder beschädigter Reputation. Im Hinblick auf die Abwehr und zur Identifikation des Nutzens entsprechender Härtungsmassnahmen wird selbstverständlich auch hier empfohlen das Instrument der Risikoanalyse unter Berücksichtigung der Wahrscheinlichkeit und des

dadurch verursachten immateriellen und materiellen Schadens einzusetzen.

E-Mail und Internet

Elektronische Kommunikation erlaubt es Social Engineers, Mitarbeitenden aus der relativen Anonymität des Internets heraus (massenweise) zu kontaktieren. Social Engineers überreden einen Mitarbeitenden eines Unternehmens durch glaubhafte List zur Preisgabe von Informationen. Diese Informationen können das Ziel des Angriffes sein oder nur ein weiterer Schritt zur Erreichung des Zieles. Die erhaltenen Informationen können unter Umständen den sich anschliessenden Malware-Angriff unterstützen oder erst ermöglichen. Deswegen müssen die Mitarbeitenden regelmässig darin geschult werden, wie sich Social Engineering-Angriffe am besten erkennen und vermeiden lassen. «Seien Sie vorsichtig!».

Viele Mitarbeitende erhalten Dutzende oder sogar Hunderte E-Mails pro Tag, sei es von Computern von Unternehmen oder Privaten. Diese Menge an E-Mails macht es heute unmöglich, jeder Nachricht die ihr gebührende Aufmerksamkeit zu schenken. Diese Tatsache kommt einem Social Engineer leider sehr entgegen.

Es ist unrealistisch zu glauben, dass Mitarbeitende den Internetzugang des Unternehmens nur für geschäftliche Zwecke verwenden, auch wenn dies unter Umständen so vorgeschrieben wäre. Die meisten Angestellten surfen auch aus privaten Gründen im Web, um etwas zu kaufen oder eigene Recherchen durchzuführen. Durch privates Surfen können die Mitarbeitenden – und damit die Computersysteme des Unternehmens – in Kontakt mit Social Engineers kommen. Selbst wenn es diese Angreifer nicht auf ein spezifisches Unternehmen abgesehen haben, könnten sie dessen Mitarbeiter dazu missbrauchen, Zugriff auf dessen Unternehmensressourcen zu erlangen.

In diesem Zusammenhang sind natürlich auch die Social Media-Plattformen zu erwähnen. Jeder Social Engineer, der etwas auf sich hält, wird versuchen, via die entsprechenden Websites Informationen zu gewinnen, die er für seine Angriffe benutzen kann. Man muss sich nur vor Augen führen, wie schnell beispielsweise unbekannte Menschen zu «Freunden» werden und auf der anderen Seite, wie unkritisch viele Benutzer solcher Sites private und/oder geschäftliche Informationen einem erstaunlich weiten Kreis zur Verfügung stellen. Das gezielte Suchen von Informationen, in diesem Zusammenhang bekannt als «Information Gathering», beispielsweise über ein Zielsystem oder eine Firma, wird oftmals unter der Verwendung von Internetsuchmaschinen gemacht. Hierbei werden natürlich auch Foren, Newsgroups oder Blogs durchsucht. Da die meisten Menschen viel zu sorglos mit ihren persönlichen Daten umgehen, ist es hier ein Leichtes, an detaillierte Informationen zu kommen. Da auch vermeintlich abgeschlossene Bereiche wie z.B. myspace.com und ähnliche durchsucht werden können, ist auch hier Vorsicht bei der Eingabe von persönlichen oder gar firmeninternen Daten geboten.

Das Telefon

Das Telefon stellt ein weiteres Angriffsmittel für Social Engineering-Angriffe dar. Es ist ein vertrautes Medium, doch es ist auch unpersönlich, da wegen der Distanz das Opfer den Angreifer nicht sehen kann. In grösseren Unternehmen kennen sich die Mitarbeitenden nicht persönlich oder es sind gar Geschäftsbereiche wie beispielsweise die IT ausgelagert. «Seien Sie auch am Telefon aufmerksam und hinterfragen Sie, welche Informationen der Anrufer von Ihnen wünscht.»

Abfälle

Das illegale Durchstöbern von Abfall ist ebenfalls ein viel versprechendes Betätigungsfeld für Angreifer. Papierabfälle in Container, die am Strassenrand stehen oder entsorgte Computer und deren Bestandteile können Informationen enthalten, die für Social Engineers von unmittelbarem Nutzen sind, beispielsweise weggeworfene Zettel mit Kontonummern und Benutzer-IDs oder Baupläne, die als Hintergrundinformationen dienen können, etwa Telefonlisten und Organisationsdiagramme. Diese Art von Informationen ist für einen Social Engineer von grösstem Wert, da sie ihn bei seinem Angriff glaubwürdiger erscheinen

lässt. Wenn der Angreifer beispielsweise gut über das Personal in einer Unternehmensabteilung Bescheid weiss, wird er wahrscheinlich erfolgreicher vorgehen können. Die meisten Mitarbeitenden werden davon ausgehen, dass jemand, der so viel über das Unternehmen weiss, selbst ein erfahrener Mitarbeiter ist, da er dadurch automatisch eine natürliche Autorität ausstrahlt.

Datenträger

Noch nützlicher können elektronische Medien sein. Wenn in einem Unternehmen keine Regeln für die korrekte Entsorgung nicht mehr benötigter Datenträger vorhanden sind, lassen sich auf weggeworfenen Festplatten, CDs und DVDs die vielfältigsten Informationen finden und dies unter Umständen in sehr grossen Mengen. Die hohe Beständigkeit fester und wechselbarer Datenträger bedeutet, dass die für IT-Sicherheit zuständigen Personen Richtlinien für die Entsorgung von Speichermedien festlegen müssen, die das Löschen der Inhalte oder die Zerstörung dieser Medien regeln.

Der Mensch selber

Am einfachsten und billigsten kommt ein Angreifer an Informationen, indem er eine Person direkt danach fragt. Diese Methode mag primitiv und allzu offensichtlich erscheinen, doch sie ist seit Urzeiten die gängigste Art des Trickbetrugs. Social Engineers haben vor allem mit den folgenden vier Methoden Erfolg:

- **Einschüchterung:** Hierzu gibt sich der Angreifer als Autoritätsperson aus, um ein Opfer dazu zu bringen, der Forderung nachzukommen.
- **Überredung:** Die gängigsten Formen der Überredungskunst sind Schmeichelei und die Erwähnung der Namen bekannter Personen (Vorgesetzte, Direktor, etc.).
- **Einschmeichelung:** Diese Methode ist meistens längerfristig angelegt: Ein untergeordneter oder gleichrangiger Kollege baut Schritt für Schritt ein Vertrauensverhältnis zum Opfer auf, um schliesslich auch Informationen von ihm zu bekommen.
- **Hilfe:** Der Angreifer bietet dem Opfer Hilfe an. Um diese Hilfe nutzen zu können, muss das Opfer letztendlich persönliche Informationen preisgeben, die der Hacker dann missbraucht.

Reverse Social Engineering

Reverse Social Engineering (umgekehrtes Social Engineering) bezeichnet eine Situation, in der die Opfer selbst den Kontakt anbahnen und dem Angreifer die gewünschten Informationen anbieten. Eine solche Situation mag abwegig erscheinen, doch Autoritätspersonen – insbesondere Personen, die hohes fachliches oder soziales Ansehen geniessen – erhalten oftmals unverlangt wertvolle persönliche Informationen wie Benutzer-IDs und Kennwörter, da sie über jeden Verdacht erhaben zu sein scheinen. Beispielsweise würde kein Helpdesk-Supportmitarbeiter eine Benutzer-ID oder ein Kennwort von einem Hilfe suchenden Anrufer verlangen. Die Probleme werden ohne diese Angaben gelöst. Viele Benutzer, die IT-Probleme haben, geben aber in der Hoffnung, dadurch die Lösung des Problems beschleunigen zu können, von sich aus diese sicherheitsrelevanten Daten an. Der Social Engineer braucht also gar nicht erst danach zu fragen.

Frage 1: Könnte man so in Ihr Unternehmen eindringen?

Durch Mitlaufen in einer Mitarbeitergruppe, die das Gebäude betreten oder so tun als sei man mit Telefonieren beschäftigt, dann den Badge-geschützten Lift betreten und warten bis der Lift in eine andere Etage gerufen wird. Oder man könnte bei Ihnen beschäftigt, telefonierend an einem anderen Ein- oder Ausgang warten, bis jemand die Tür öffnet und diese dann für den unberechtigten Zutritt nutzen?

Weitere Beispiele zu ähnlichen Szenarien gäbe es viele!

Frage 2: Können Sie sicher sein, dass Ihre Mitarbeitenden die folgenden Punkte einhalten?

Alle Mitarbeitenden und Besucher tragen den Badge immer gut sichtbar. Die Clear Desk Policy wird ausnahmslos eingehalten. Auf mobilen Geräten werden vertrauliche Informationen immer nur verschlüsselt gespeichert. USB-Sticks können nur sehr beschränkt an Ihre Computer angeschlossen werden. Vertrauliche Informationen werden richtig und sicher entsorgt, usw.

Wenn Sie sich bei der Beantwortung der obigen Aussagen nicht sicher sein können, sollten Sie sich überlegen, Ihre getroffenen Sicherheitsmassnahmen durch eine externe Fachstelle überprüfen zu lassen und deren Umsetzung zu auditieren.

Bei der Swiss Infosec AG wird Social Engineering als eine Auditmethode nur im Auftrag eines Unternehmens durchgeführt und dies mit dem Ziel, die Infrastruktur und Mitarbeitenden des jeweiligen Unternehmens zu schützen.

Jede Unternehmung hat ein elementares Interesse (Image, Konkurrenzvorsprung, Risk Management, Qualitätsmanagement) ihre Informationen, die nicht für die Öffentlichkeit bestimmt sind, vor unberechtigtem Zugriff zu schützen. Auf der anderen Seite wird entsprechend durch Gesetzesbestimmungen vorgegeben, dass bestimmte Informationen, insbesondere schützenswerte oder besonders schützenswerte Personendaten, einer speziellen Behandlung bedürfen.

Das Management und alle verantwortliche Personen sind ausserdem gefordert, die an sie gestellten Anforderungen und Ziele bezüglich der Sicherheitssensibilisierung der Mitarbeitenden zu erfüllen – auch im Sinne einer Vorbildfunktion.

Ein Social Engineering-Audit

Diese Auditmethode ist die am besten geeignete Methode, um festzustellen, inwieweit die notwendigen, intern definierten oder beabsichtigten «weichen» mitarbeiterbezogenen Regeln in der Praxis effektiv wirken und beachtet werden. Oder in anderen Worten: Mittels eines Social Engineering-Audits erhält eine Organisation Steuerungsinformation zum aktuellen Niveau der Awareness und der Umsetzung fundamentaler Sicherheitsregeln. Ein hervorzuhebender Nebeneffekt ist, dass die involvierten Stellen bzw. Personen gleichzeitig und sehr effektiv sensibilisiert werden. Ein Social Engineering Audit lässt sich in unterschiedlichstem Umfang und Tiefe durchführen.

Phasen eines Social Engineering-Audits

In einer ersten Phase werden die Anforderungen seitens der Organisation aufgenommen, die Vorgaben für die Abwicklung festgehalten sowie das Einsatzgebiet definiert und dokumentiert. In einem nächsten Schritt werden die Auditobjekte festgelegt, dabei wird unterschieden zwischen Auditobjekten in fachlicher und in geografisch-organisatorischer Hinsicht.

Fachliche Auditobjekte und -bereiche können hierbei sein: Informations- und IT-Sicherheit allgemein, sprich technisch, organisatorisch, personell (beispielsweise Ausbildungsstand), rechtlich, physisch (Zutrittsschutz zu Rechenzentrum, Personalakten, Datenschutz). Oder spezifische Audits in Bezug auf einen Vorfall, ein aktuelles Problem, Benutzerfreundlichkeit, Umsetzungsgeschwindigkeit, Machbarkeit, Wirtschaftlichkeit, Akzeptanz von Vorgaben, etc.

Im Rahmen eines Social Engineering-Audits können aber auch spezifische Punkte überprüft werden wie z.B.: Wo existieren ungeschützte Informationen, Netzverbindungen, Dokumente, Datenzugriffe, usw. Diese Auflistung ist nicht abschliessend und selbstverständlich den jeweiligen Erfordernissen des Unternehmens anzupassen.

In geografisch-organisatorischer und zeitlicher Hinsicht können mit einem Social Engineering-Audit unter anderem folgende Punkte überprüft werden: Unterschied von Geschäftsbereichen in nationaler und internationaler Hinsicht, bestimmte Tochtergesellschaften oder Organisationseinheiten. In diesem Zusammenhang kann auch flächendeckend auditiert werden oder man konzentriert sich im Rahmen des konkreten Auftrages auf Stichproben bzw. Teilgebiete oder das Audit wird während oder ausserhalb der Bürozeiten durchgeführt oder nur an bestimmten Arbeitstagen.

Vorgehensweise

In Phase II werden spezifische Informationen, je nachdem, ob der Auftraggeber einen Black, White oder Grey Box-Ansatz gewählt hat, betreffend des Social Engineering-Audits zwischen der Auftraggeberin und dem Auditor ausgetauscht und dokumentiert. Folgende Angriffsformen lassen sich kombinieren: Information Gathering (u.a. telefonisch, persönliche Gespräche vor Ort); Begehung, Zutritt und Aufenthalt im Gebäude; Phishing und Ethical Hacking (WLAN); Ausnutzung situativer Gelegenheiten; Einschleichen, Lügen, Erschleichen, Täuschen, Entwenden, usw. sowie der Einsatz von Keyloggern, Kameras, Tonbändern, Kopierern, usw.

In diesem Zusammenhang ist es wichtig darauf hinzuweisen, dass sämtliche Aktionen vorgängig seitens der Auftraggeberin im Detail bewilligt werden.

Das Social Engineering-Audit

In Phase III wird aufgrund der in Phase I abgesprochenen Vorgehensweise der aktuelle Stand festgehalten und das Sicherheitsverhalten im Unternehmen getestet. Solche Audits werden nur unter der Voraussetzung durchgeführt, dass sich ein Ansprechpartner des Auftraggebers vor Ort befindet, der kontaktiert werden kann, sollte eine Deeskalation erforderlich sein.

Vereinfacht kann man zwischen den folgenden Typen von Social Engineering-Audits unterscheiden:

Standard

Beim Standard Social Engineering-Audit wird mit Hilfe technischer Kommunikationsmittel (wie Telefon, E-Mail) versucht, vom Angesprochenen Informationen zu erhalten, ohne dass diese weitergeleitet werden bzw. der Anfragende identifiziert wird. Unter diesen Umständen geben wir uns unter anderem als Systemadministrator, Sicherheitsbeauftragter, Helpdesk-Mitarbeiter oder Mitglied der Geschäftsleitung aus.

Advanced

Mit dem Advanced Social Engineering-Audit wird zusätzlich versucht, direkt auf die entsprechenden Zielpersonen respektive Zielobjekte zuzugehen, sei dies als Handwerker oder Mitglied einer Putzequipe, als neuer Mitarbeiter oder auch als Mitarbeiter der IT-Abteilung.

Individual

Das Individual Social Engineering-Audit ist ein mit dem jeweiligen Unternehmen individuell zusammengestelltes Vorgehen, unter Berücksichtigung spezieller Wünsche und Bedürfnisse. Jedoch ist in diesem Zusammenhang darauf hinzuweisen, dass hierbei keine Vorgehensweise unterstützt wird, die gegen den Persönlichkeitsschutz verstossen könnte. Auch ist es hierbei unabdingbar, das Vorgehen im Detail zu besprechen, damit generell ein widerrechtliches Handeln ausgeschlossen werden kann. Aus diesem Grunde lassen wir uns vom Auftraggeber auch immer eine schriftliche Einverständniserklärung bezüglich der Vorgehensweise geben.

Auswertung und Resultate

Die während dem Audit gesammelten Daten werden ausgewertet und analysiert. Dabei darf das Vertrauensverhältnis zwischen Arbeitnehmer und Arbeitgeber nicht gestört werden. Deswegen wird auch grosser Wert darauf gelegt, dass in den Auswertungen alle Hinweise auf spezifische Personen neutralisiert werden, es sei denn, es fänden sich Hinweise auf illegale Tätigkeiten.

Massnahmen und Konzepte

Die Auditauswertung führt, basierend auf dem Analysebericht, zu einem Massnahmenkatalog mit Vorschlägen zur Korrektur der festgestellten Schwachstellen.

ZUSAMMENFASSUNG

- Social Engineering ist eine Angriffsform, die die Schwachstelle Mensch ausnutzt
- Social Engineering-Audits dienen der Überprüfung der Umsetzung und Einhaltung von Regeln und der Wirksamkeit von Aus- und Weiterbildungen.

Ziel und Zweck eines Social Engineering-Audits

- Beschaffung von Steuerungswissen über die firmenweite Verbreitung und Umsetzung von Sicherheitsmassnahmen
- Sensibilisierung und Verhaltensüberprüfung aller Beteiligten
- Begründung und Herleitung von Optimierungsmassnahmen
- Mögliche Betriebsunterbrüche verhindern
- Ihr Image und Vertrauen stärken
- Ihre Konkurrenzfähigkeit und Wettbewerbsvorteile ausbauen

Ein Social Engineering-Audit liefert Antworten unter anderem zu folgenden Fragen:

- Wie stark ist unsere Sicherheitskette und wo sind ihre Schwachstellen?
- Was muss passieren, damit wegen einer sicherheitsrelevanten Situation der Sicherheitsdienst alarmiert wird?
- Wie verhalten sich die beteiligten Mitarbeitenden, wenn eine sicherheitsrelevante Situation erkannt wird und wie reagiert der Sicherheitsdienst?

DER AUTOR

Reto C. Zbinden,
Rechtsanwalt, CEO
Swiss Infosec AG
Centralstrasse 8A
6210 Sursee
+41 (0)41 984 12 12
infosec@infosec.ch

Information des Verbandes

CISA – das Personenzertifikat für IT-Prüfer

CISA ist das älteste und wohl bekannteste der vier ISACA-Personenzertifikate: bereits über 89,000 Personen haben seit 1977 den »Certified Information Systems Auditor" erworben. Im Abstand von jeweils 4–6 Jahren wurde das Berufsbild an die Entwicklungen der Informationstechnologie und der anspruchsvollen Tätigkeit des IT-Prüfers angepasst – letztmals auf die Prüfung im 2011. Das CISA-Zertifikat umfasst derzeit fünf Domains, 38 Tasks (Aufgaben) und 80 Knowledge Statements (Aussagen zum benötigten Fachwissen). Da die Task Statements auf die jeweiligen COBIT-Prozesse referenziert sind, wird COBIT de facto zu einem integrierenden Bestandteil der CISA-Ausbildung und -Zertifizierung.

Für das CISA-Zertifikat muss eine vierstündige Prüfung bestanden werden; zudem sind fünf Jahre qualifizierte Fachpraxis nachzuweisen, wobei bestimmte Tätigkeiten, Abschlüsse und Titel mit bis zu max. drei Jahren angerechnet werden können.

Ein Blick auf das Berufsbild zeigt die Breite der Tätigkeit eines CISA: Während im ersten Domain die Grundlagen der IT-Prüfungstätigkeit definiert werden, umfassen die anderen Domains die verschiedenen Facetten der Informatik (IT): Governance und Führung der IT, Lebenszyklus-Management von Anwendungen und Infrastruktur, Auslieferung und Unterstützung von IT-Dienstleistungen, Schutz von Informationswerten (Assets). Für jedes der Fachthemen aus dem CISA-Berufsbild sollte ein Kandidat die jeweiligen Risiken und Sicherheitsmassnahmen verstehen und zudem eine entsprechende Prüfung durchführen können.

Das ISACA Switzerland Chapter führt zwei Mal jährlich einen berufsbegleitenden Kurs (15 Kurstage verteilt über jeweils 4–5 Monate) durch. Dieser richtet sich an alle Personen, die Interesse an der Prüfung, Kontrolle und Sicherheit von Informationssystemen haben, und ist nicht an das Ablegen der CISA-Prüfung gebunden. Ebenso ist der CISA-Kurs keine Vorbedingung für die Teilnahme an der offiziellen CISA-Prüfung. Vorbedingung für die Kursteilnahme ist hingegen eine ein- bis zweijährige «qualifizierte» Berufspraxis sowie umfassende Informatik-Kenntnisse.

Der CISA-Kurs richtet sich an alle Personen, die sich mit der Sicherheit, Kontrollierbarkeit und Ordnungsmässigkeit von Informationssystemen beschäftigen – neben den internen oder externen IT-Prüfern sind dies vor allem IT-Sicherheitsbeauftragte, Compliance-Officer, IT-Projektleiter oder Projektcontroller und viele andere mehr. Die Teilnehmer sollten zudem am Bestehen der CISA-Prüfung interessiert sein, was jedoch keine Voraussetzung für den Kursbesuch ist.

WEITERE INFORMATIONEN

Weitere Details zum CISA-Zertifikat und zur entsprechenden Ausbildung finden Sie auf www.isaca.ch

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
9.12.11-8.5.12	CISA-VK	**CISA-Zertifikatskurs 2012|1:** Vertiefungskurs IT-Revision, IT-Kontrolle, IT-Sicherheit, IT-Governance und CISA-Prüfungsvorbereitungskurs. Offizieller CISA-Kurs des ISACA Switzerland Chapter
9.12.11-9.5.12	CISM-VK	**CISM-Zertifikatskurs 2012|1:** Vertiefungskurs Konzeption, Governance und Management der Informationssicherheit, Risiko-Management, Reaktionsmanagement und CISM-Prüfungsvorbereitungskurs. Offizieller CISM-Kurs des ISACA Switzerland Chapter
9.12.11-10.5.12	CGEIT-VK	**CGEIT-Zertifikatskurs 2012|1:** Vertiefungskurs IT-Governance: strategische Ausrichtung, Wertschöpfung, Risikomanagement, Ressourcen-Management und Leistungsmessung und CGEIT-Prüfungsvorbereitungskurs. Offizieller CGEIT-Kurs des ISACA Switzerland Chapter
9.12.11-11.5.12	CRISC-VK	**CRISC-Zertifikatskurs 2012|1:** Vertiefungskurs Identifikation, Management und Überwachung von (IT) Risiken, Einführung, Betrieb und Überwachung des IKS und CRISC-Prüfungsvorbereitungskurs. Offizieller CRISC-Kurs des ISACA Switzerland Chapter
12.-13.12.11	COB-IG	**ISACA Implementing Governance of Enterprise IT Using COBIT**
19.-21.3.2012	COB-FB	**ISACA COBIT 4.1 Foundation Zertifikat**
18.-19.6.2012	COB-FB	**ISACA COBIT 4.1 Foundation Zertifikat**

Das gesamte Trainingsangebot mit näheren Informationen finden Sie online unter www.isaca.ch

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
Erscheinungsweise: 4x jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch

Copyright: © Switzerland Chapter der ISACA