Härtetests für Unternehmen

Marktübersicht Da Sicherheit für fast jeden Bereich der IT relevant ist, müssen Security Audits und Assessments alle Bereiche der Informationssicherheit abdecken. Angebote gibt es viele, die folgende Marktübersicht soll bei der Auswahl helfen.

Von Simon Wegmüller

Unternehmenskritische Business-Prozesse sind heute meist stark von IT-Prozessen und der IT-Infrastruktur abhängig. Es ist deshalb für Unternehmen zentral zu wissen, dass ihre sicherheitsrelevanten Systeme hinreichend geschützt sind. Dieses Bedürfnis führt oft dazu, dass sie ihre Systeme durch einen externen Dienstleister prüfen lassen.

Solche Angebote beinhalten zumeist Audit- und Assessmentkomponenten, sowohl für CIOs als auch für Security-Verantwortliche, Compliance Leads oder Verantwortliche für die interne Revision.

«Den Scope der Security Audits richten wir auf die individuellen Erfordernisse dieser Anspruchsgruppen aus, etwa die Beurteilung eines bestehenden Security-Risikos, die Begutachtung einer Cybersecurity-Strategie für Verwaltungsrat und Geschäftsleitung oder die konkrete Evaluation der Plattformsicherheit», erklärt etwa Adrian Marti, Partner und Head Cyber Security & Privacy AWK Group, und konkretisiert: «Übergreifend besteht der Wunsch, eine unabhängige Aussensicht sowie bei festgestellten Defiziten konkrete Empfehlungen zur Behebung zu erhalten. Unabhängig heisst: sowohl frei von organisatorischen Bindungen zum Auftraggeber als auch neutral hinsichtlich von Serviceanbietern und Lieferanten.»

Audit vs. Assessment

Die meisten Unternehmen sind besonders daran interessiert, an Empfehlungen zur Verbesserung der eigenen Cyber-Resilienz zu gelangen. Diese können sowohl technischer Natur sein und beispielsweise mit Penetration Tests ermittelt werden, oder auch organisatorisch respektive Prozess-orientiert. Die meisten Unternehmen unterscheiden dabei zwischen einem Audit und einem Assessment.

Ein Audit bezieht sich dabei grundsätzlich auf die systematische und intelligente Prüfung der Cybersicherheit. Der Audit untersucht, ob Prozesse, Anforderungen und Richtlinien die geforderten Standards (beispielsweise ISO 27001, NIST, IKT Minimalstandard usw.) erfüllen. «Die zu Grunde liegende Frage ist meist: wo erfülle ich den Standard und wo besteht Optimierungspotenzial», erklärt Markus Limacher, Head of Security Consulting bei Infoguard.

Ein Security Assessment dient derweil in erster Linie der Ermittlung von IT-Sicherheitslücken und -risiken. «Die zu Grunde liegende Frage hier ist meist: wie und wo kann ich mich am effektivsten verbessern», so Limacher weiter.

Doch wann und wieso benötigt ein Unternehmen einen IT-Audit und wann reicht eine unabhängige Sicherheitsanalyse in Form eine Assessments durch einen externen Dienstleister?

«Ein externer und unabhängiger Berater arbeitet unvoreingenommen und kann Risiken identifizieren, die für Mitarbeitende unter Umständen gar nicht mehr wahrnehmbar sind – Stichwort Betriebsblindheit», erläutert dazu Christoph Baumgarter, CEO des Unternehmens Oneconsult. «Nicht zuletzt gilt leider im Alltag oft die Devise, dass der Prophet im eigenen Land nicht viel zählt – selbst wenn er mit allen Aussagen richtig liegt.»

Zudem seien solche IT-Infrastruktur- und -Sicherheitsanalysen für die Spezialisten Alltag, denn diese wissen aufgrund ihrer Erfahrung genau, welche Schwachstellen in der Praxis ausgenutzt werden und welche eher theoretischer Natur sind.

Vorbereitung seitens Unternehmen

Die Vorbereitung eines Audits oder auch Assessments wird zumeist in einem Vorgespräch besprochen. Bei Interview-basierten Assessments ist es, so sind sich die Anbieter einig, unabdingbar, dass Interviewpartner rechtzeitig genügend Zeit reservieren. «Bei technischen und praktischen Sicherheitsprüfungen erhalten Kunden den besten Nutzen einer Sicherheitsprüfung, wenn von Tag eins einer Prüfung ein Testen unter möglichst realen Bedingungen möglich ist», verrät etwa Martin Schobert, Geschäftsführer von Pentagrid. Mitunter kann die Vorbereitung schon im Einkaufsprozess beginnen. Wenn eine Firma einen Service durch Dritte entwickeln lässt und die Unterstützung für Sicherheitsanalysen nicht bereits in der Vertragsphase geklärt ist, können sich Möglichkeiten für spätere praktische Sicherheitstests reduzieren. Dass kann den Zugriff auf Source Code für eine Detailprüfung betreffen und wer für die Kosten von Problembehebungen aufkommt. Ähnlicher Meinung ist auch Sven Vetsch, Partner bei Redguard: «Am wichtigsten ist es, sich bewusst zu werden, was mit dem Audit erreicht werden soll. Abhängig von den zu erreichenden Zielsetzungen gibt es unterschiedliche Audit- und Testverfahren. Auf keinen Fall sollte versucht werden, einem Auditor oder Security Tester bekannte Sicherheitsprobleme vorzuenthalten oder das Auffinden solcher zu erschweren, da so eine realistische Gesamtsicht verunmöglicht wird und potenziell unternehmenskritische Risiken später nicht adressiert werden können.»

Und auch das Bewusstsein um das eigene Risiko und den Wert der Integrität

der eigenen Daten- & IT-Infrastruktur sollten Unternehmen nicht unterschätzen. «Oft sind sich KMU nicht bewusst, welche Risiken die eigene IT birgt», verrät Reto Baschera, Leiter Geschäftsfeld KMU von Swisscom. «Ein Security Assessment bietet sich daher stets an, um die Ausgangslage zu erfassen. Ein Assessment empfiehlt sich aber auch nach Änderungen in der IT-Landschaft, wie zum Beispiel der Einführung von Home Office, da mit neuen Arbeitsweisen andere Rahmenbedingungen einhergehen und entsprechend ganz andere Sicherheitsproblematiken auftreten können.»

Nachfrage kommt aus allen Branchen

«Durch die rasche Digitalisierung ist die Nachfrage branchenübergreifend», verrät derweil Senior Cyber Security Advisor Gaetano Maito der Wizlynx Group. «Unsere Kunden sind primär aus den Branchen Chemie & Pharma, Banken & Finanzen, Telekommunikation, Energie & Umwelt, aber auch Gesundheitswesen oder Handel. Wenn man das thematisch betrachtet, wären das Web Applikationen, Infrastruktur, Cloud, Entwicklung / Code, IoT, kritische Infrastrukturen, Industrial

17 ANBIETER VON SECURITY AUDITS UND ASSESSMENTS

ANBIETER	ADNOVUM	ADVACT	AWK GROUP	CISS
Anzahl Mitarbeiter in der Schweiz	360	8	400	4
Angebot richtet sich an	alle Branchen, KMU bis grosse Unternehmen	k.A.	alle Branchen	alle Branchen, alle Firmengrössen
Kurzbeschreibung Security Audits	Security Audits sind ähnlich aufgebaut wie ein Security Assessment. Der Fokus liegt bei Security Audits jedoch auf der Erfüllung der Vorgaben für eine gewünschte Zertifizierung.	ganzheitliche Security Audits für KMU; Resultate in Form von konkret vorgeschlagenen Massnahmen	AWK unterstützt mit dem Bereich «tech-driven Audits» Kunden in der Durchführung von Audits für eine Vielzahl regulatorischer und gesetzlicher Security-Vorgaben.	Evaluation des aktuellen Stands der Informationssicherheit für Unternehmen. Basierend auf ausgewählten Standards wird der genaue Prüfungsumfang (Breite und Tiefe) mit dem Kunden im voraus vereinbart.
Standards	ISO 27001/27002 (PCI-DSS und andere ISO-Standards auf Anfrage)	k.A.	NIST SP 800-53, ISO 27001	ISO27001/2/5, IKT Minimalstandard Schweiz, GDPR, DSG und COBIT
Kurzbeschreibung Security Assessment	Ein Cyber-Security Assessment umfasst eine Definition der Vorgaben, eine Analyse der Ist-Situation, eine Gap-Analyse zur Soll-Situation inklusive Risikoermittlung und -beurteilung sowie einen finalen Report mit einer Liste von priorisierten Massnahmen.	siehe Kurzbeschrieb Security Audit	AWK bietet Security-Assessmentleistungen angefangen bei der Cyber-Strategie und bei Security-Prozessen (CSIRT, SIEM, SOC etc.) über Security-Team- und Skillstrukturen bis hin zur operativen Umsetzung der Vorgaben und Pen-Tests an.	Sicherheitsexperten prüfen das Design und die Architektur auf Schwachstellen, identifizieren und analysieren diese. Es werden Massnahmen zur Verbesserung des Sicherheitskonzeptes festgelegt. Ziel dieses Assessments ist es, festzustellen, ob die vorhandenen Sicherheitsressourcen/-massnahmen ausreichend sind und welche Massnahmen zur Verbesserung ergriffen werden müssen.
Kurzbeschreibung Penetration Test	Hackerangriffe auf eigene IT-Systeme, um auf objektive Weise Schwachstellen zu identifizieren und zu beheben. Nach dem Test erhält das Unternehmen einen ausführlichen Bericht, der die identifizierten Schwachstellen und ihre Bedeutung und Kritikalität beschreibt und Massnahmen zu ihrer Behebung empfiehlt.	Evaluation der Angriffsfläche von Aussen	Aufgrund der Vielzahl an Technologien und Pen-Test-Varianten wird ein Partner-Ökosystem genutzt, um eine breite Palette anbieten zu können.	Ziel des Penetration Test ist es, die IT-Systeme und/oder Netzwerke einer umfassenden Prüfung zu unterziehen um festzustellen, welche Schwachstellen die Systeme in Bezug auf echte Angreifer/Hacker haben. Es werden ähnliche Techniken und Methoden, die von echten Angreifern/Hackern eingesetzt werden, verwendet, um unbefugten Zugriff auf die Systeme zu erhalten.
Preismodell	Fixpreis oder nach Aufwand	nach Aufwand und Komplexität	nach Aufwand und Komplexität	Fixpreisofferte nach Festlegung des Umfangs mit dem Kunden
Kosten	auf Anfrage	ab Fr. 5000.–	nach Aufwand und Komplexität	ab Fr. 2400.–
Info	www.adnovum.ch	www.advact.ch	www.awk.ch	www.360incontrol.ch

■ = ja, ❑ = nein; k.A = keine Angaben

Control Systems (ICS) und Operational Technology (OT) und so weiter.» Dem pflichtet unter anderem auch Dragisa Mitrovic, Senior Security Consultant bei T-Systems Schweiz, bei: «Aus unserer Perspektive kommt die Nachfrage relativ gleichmässig aus allen Branchen.»

Die Kosten-Frage hingegen lässt sich nicht ganz so einfach beantworten, da dabei viele verschiedene Faktoren zum Tragen kommen. «Die Kosten hängen stark vom Umfang ab», so Jason Marsch, Head of Security Assessments and Projects bei Swiss IT Security. «Wir bieten unseren Kunden unterschiedliche Audit- und Assessment- sowie Penetration-Testing-Module an, welche einzeln oder in Kombination eingesetzt werden können.»

Im Vorfeld eines Projektes werden mit dem Kunden deshalb üblicherweise der Scope des Audits oder Assessments definiert und daraus die nötigen Module und Modulkonfigurationen gewählt, dies ergibt dann die Kosten. Diese Strategie wird so von den meisten hier aufgeführten Unternehmen verfolgt. Die meisten Prüfungen dauern dabei zwischen fünf und fünfzehn Personentagen. ■

Fortsetzung Marktübersicht auf den folgenden Seiten ➤

FIRST SECURITY TECHNOLOGY	INFOGUARD	INFOSEC	ISECURE
k.A.	150	38	5
alle Branchen, KMU	alle Branchen, Fokus Schweiz Top 500 Unternehmen & regulierte Unternehmen	alle Branchen, alle Unternehmensgrössen	alle Branchen, KMU, Kleinbetriebe
siehe Kurzbeschrieb Security Assessment	gezielte Sicherheitsüberprüfungen, Security Audits und Asssessments sowie Penetration Tests zur Verifikation von Sicherheitsprozessen, der IT-Infrastruktur sowie der Mitarbeitenden	Audits und Assesments in den Bereichen Integrale Sicherheit, Informationssicherheit, IT-Sicherheit und Datenschutz	ICT-Audit nach der EISA-Methode, technische und organisatorische Aspekte; Interviews (mehr als 20 Fragenbereiche), Stichproben, Überprüfung mit Tools und, wenn gewünscht, Penetration Tests.
ISO 27001, ISO/IEC 29147, ISO/IEC 27032, ISO 9001, ISO/IEC 27017, ISO 22301, ISO 31000, ISO/IEC 20000	ISO 27001, ISO 22301, NIST, IKT Minimalstandard, SWIFT	ISO 27001, ISO 27002, ISO 27701, ISO 22301, NIST Cyber Security Framework, IKT-Minimalstandard BWL, OWASP, CIS, u.w.	ISO 27001, ITIL, IT-Grundschutzmodel
vollautomatisierte Analyse der gesamten IT-Infrastruktur inklusive Inventar und Massnahmenkatalog	Security Assessments zu verschiedenen Themen wie: NIST CSF, IKT Minimalstandards, SWIFT, Backup& Recovery, BCM, Cyber Resilience, etc.	siehe Kurzbeschrieb Security Audit	massgeschneiderte Assements in Absprache mit dem Auftraggeber; Beurteilung aufgrund von Interviews und schriftlichen Unterlagen
vollautomatisierte und regelmässige Analyse der gesamten IT-Infrastruktur auf IT-Schwachstellen (Vulnerability Management)	Penetrations-/Vulerability-Testing in verschiendenen Ausrpägungen, wie Attack Simulationen, Red Teaming, Purple Teaming, etc.	Identifizierung von Schwachstellen in Web- oder Mobileapplikationen oder in Netzwerken innerhalb eines definierten Scope	massgeschneiderte Penetration Tests in Absprache mit dem Auftraggeber, diese können alle Facetten von Eindringversuchen beinhalten
basierend auf Anzahl der zu prüfenden Systeme	auf Anfrage	auf Anfrage	Offerten nur aufgrund von Vorgesprächen und Abklärungen
ab Fr. 580.–	auf Anfrage	auf Anfrage	Offerten
www.first-security.com	www.infoguard.ch	www.infosec.ch	www.isecure.ch

Quelle: «Swiss IT Magazine»

SECURITY-AUDIT-ANBIETER (FORSETZUNG)

ANBIETER	NOMASIS	ONECONSULT	PENTAGRID	REDGUARD
Anzahl Mitarbeiter in der Schweiz	18	41	3	50
Angebot richtet sich an	alle Branchen und Unternehmen	alle Branchen, alle Unternehmensgrössen vom KMU bis zu Grosskonzern	alle Branchen	alle Branchen und Unternehmensgrössen, Fokus DACH-Region
Kurzbeschreibung Security Audits	siehe Kurzbeschrieb Security Assessment	Anhand von Dokumentenreviews, Fragebogen und (strukturierten) Interviews wird das Sicherheitsniveau des Untersuchungsobjekts (z.B. Rechenzentrum, Abteilung, Standort oder Gesamtorganisation) von zertifizierten Auditoren ermittelt, üblicherweise in Form eines Spinnennetzdiagramms visualisiert und entsprechende Massnahmen- und Priorisierungsempfehlungen im Schlussbericht abgegeben. Die Überprüfung orientiert sich an den einschlägigen Normen (ISO, BSI, Common Criteria, NIST, IKT-Minimalstandard etc.) und wird auf die individuellen Bedürfnisse des Kunden angepasst.	siehe Kurzbeschrieb Security Assessment	Überprüfung der Erfüllung von gesetzlichen und regulatorischen Anforderungen aus den Bereichen Informationssicherheit sowie Datenschutz; bei Bedarf Aufbau der Ergebnisse oder Überführung in ein Managementsystem
Standards	k.A.	ISO 270xx, BSI, Common Criteria, NIST, IKT-Minimalstandard etc.	OWASP (Mobile & Web), BSI/NIST/CIS, ISO 2700x, UL 2900 u.w.	ISO 27001, ISO 27002, ISO 27701, BSI IT-Grundschutz, PCI-DSS, IKT-Minimalstandard, OWASP, PTES, NIST, revDSG, GDPR, SWIFT, (nicht abschliessend)
Kurzbeschreibung Security Assessment	Praxisbezogene Überprüfung der Sicherheitseinstellungen, Konfigurationen, Richtlinien und der Abwehrmechanismen zum Schutz vor mobilen Bedrohungen und eine dokumentierte Zusammenfassung mit empfohlenen Kontrollmechanismen (Best Practices) sowie eine Abschlusspräsentation	Kombination von konzeptionellen Überprüfungen (Interviews, Review von Dokumenten etc.) und technischen Hands-on-Tests (Penetration Tests, Architekturreviews, Überprüfung von Konfigurationen etc.).	technische Analyse von Software, Hardware, Netzwerken und Infrastruktur sowie Review von Konzepten und Prozessen	Beurteilung des Cyber-Security-Dispositivs. Auf der Basis dieser Ergebnisse werden gezielte Massnahmen auf verschiedenen Ebenen zum Schutz vor Cyber-Angriffen definiert und umgesetzt. Die Grundlage dazu stellt das NIST Cyber Security Framework.
Kurzbeschreibung Penetration Test	nicht verfügbar	verschiedene Typen von Red Teaming Tests / Penetration Tests , ausgerichtet auf die spezifischen Anforderungen von Web-Applikationen, Mobile Apps, Industriesteuerungssystemen, IoT-Geräten, diversen Angriffsvektoren und Rahmenbedingungen oder die individuellen Kundenwünsche	Penetration Tests von Softwaresystemen, Hardware, Netzwerken und Infrastruktur im White- bis Black-box-Verfahren	Prüfung durch aktive Angriffe eines definierten Scope (z.B. Netzwerksegmente, Server, Applikationen) auf Schwachstellen.
Preismodell	nach Aufwand	Verrechnung nach Aufwand (Arbeitsstunden)	Kosten nach Zeitaufaufwand, Kontingente sind möglich	nach Aufwand oder pauschal
Kosten	auf Anfrage	ab Fr. 5000.–	marktüblicher Tagessatz	durchschnittlich ca. Fr. 8000.– bis Fr. 15'000.–
Info	www.nomasis.ch	www.oneconsult.com	www.pentagrid.ch	www.redguard.ch

■ = ja, ❑ = nein; k.A = keine Angaben

SWISS IT SECURITY GROUP	SWISSCOM	TERREACTIVE	T-SYSTEMS	WIZLYNX GROUP
120	k.A.	70	42	25
KMU und Grossunternehmen	alle Branchen, KMU	alle Branchen, Firmen ab 10 Mitarbeiter	alle Branchen, KMU	alle Branchen, KMU
Modularer Audit Service bestehend aus klassischen Audits, Assessments in verschiedenen Bereichen sowie Penetration/Vulnerability Testing. Der Kunde wählt die benötigten Module aus.	siehe Kurzbeschrieb Security Assessment	Audits sind so konzipiert, dass sie Technologie, Prozesse und Menschen als Teil einer Organisation bewerten. Ziel ist es, dem Kunden die in der Organisation bestehenden Risiken aufzuzeigen und eine Liste möglicher Abhilfemassnahmen zu empfehlen, um diese zu priorisieren.	T-Systems ist kein akkreditierter ISO 27001 Auditor – unterstützt jedoch bei Vorbereitung auf Erst-/Re-Zertifizierungen, GAP-Analysen und interne Pre-Audits	Sicherheitsbewertungen und Penetration Tests, umfassende Analysen von Schwachstellen und entdecken von Schwachstellen, die während der Bewertungs-Projektlaufzeit identifiziert und ausgenutzt werden konnten
ISO 2700x, BSI IT-Grundschutz, PCI-DSS, NIST CSF, COBIT u.w.	alle gängigen Security Standards wie NIST, ISO27001, BSI usw.	k.A.	ISO 27001 (ISMS) / ISO 22301 (BCM) / ISO 27017/27018 (Cloud) / Datenschutz (DSG/ DSGVO)	CREST Global zertifiziert
Assessments sind modular aufgebaut und decken folgende Bereiche ab: Security Overview, Security Deep Dive, Firewall, Microsoft 365, Microsoft Teams, Datenschutz. Unsere Assessments zeigen Sicherheitslücken und Schwachstellen auf sowie konkrete Massnahmen und Empfehlungen zur Schliessung dieser.	Das Assessment umfasst strukturierte Interviews sowie einen softwarebasierten Scan der ICT-Umgebung (Vulnerability Scan) durch unsere Experten. KMU erhalten einen ausführlichen Abschlussbericht inkl. Massnahmenkatalog zur Verbesserung der IT-Sicherheit, einen Inventarbericht der ICT-Infrastruktur sowie eine Risikoeinschätzung der identifizierten Schwachstellen und fehlerhaften Konfigurationen.	Ein technisches Assessment testet die Technologie-Implementierungen, mit einem Überblick über die Prozesse. Das Ziel ist, Schwachstellen zu entdecken und deren Auswirkungen auf die betroffenen Systeme zu verstehen.	Das Assessment ist modular aufgebaut und beinhaltet eine vielzahl von Überprüfungen, interne Secuity-Prozesse werden gegenüber ISO 27001, NIST Cybersecurity Framework oder an IKT Minimalstandard bewertet, dazu kommen versch. Reviews, z.B. Architektur-/Netzwerkdesign sowie Reviews von Konfigurationen von Security- und Netzwerkgeräten in der IT wie auch Industrial Security (OT).	vier Phasen: Informationsbeschaffung, Schwachstellen-Identifizierung, Ergbnis-Analysen und Berichtserstattung
Neben den externen und internen Penetration Tests werden spezifische Tests für Web Application und SCADA Produktionssysteme angeboten. Auch Targetted Attacks/Client Side Penetration Tests und Social-Engineering-Angriffe werden ausgeführt.	Der Vulnerability-Scan ist im Security Assessment inkludiert. Nebst der Möglichkeit eines Vulnerability-Scans bietet Swisscom Kunden einen vollumfänglichen Pentesting Service an.	Penetration Test für enges Budget wahlweise mit Schwerpunkt Intrusion für externe technische Betrachtung oder Resilience (Angreifer befindet sich schon im Firmennetz). Test nach OWASP-Top-10 für Webapplikationen. Oder umfassender Penetration Test für Netzwerk.	Penetration Tests von Webapplikationen und Netzwerken wie auch SAP-Systemen, welche entweder Remote oder aber vor Ort durchgeführt werden können. Diese können in versch. Ausprägungen angeboten werden, z.B. als Black- oder Greybox-Tests. Ein Schwachstellen-Scan ist immer inkludiert im Service, kann aber auch einzeln Angeboten werden.	Penetration-Test-Vorgehensweise basierwend auf dem Ansatz, der im OWASP Testing Guide, Open Source Security Testing Methodology Manual (OSSTMM) und Penetration Testing Execution Standard (PTES) beschrieben ist.
modular aufgebaut, wiederkehrende Tests auf Subscription-Basis möglich	pauschal	3 standardisierte Basisangebote zum Fixpreis sowie zahlreiche kundenspezifische Angebote	nach Aufwand und Komplexität	nach Aufwand und Komplexität
nach Aufwand und Komplexität	Security Assessment für KMU: Fr. 4200.– (pauschal); Pentesting (offertenbasiert)	nach Aufwand und Komplexität	ab Fr. 7500.–	ab Fr. 2500.–
www.sits.ch	www.swisscom.ch	www.terreActive.ch	www.t-systems.com	www.wizlynxgroup.com

Quelle: «Swiss IT Magazine»