

Vertrauen zu externen IT-Beratern?

IT-Sicherheit mit Drittanbietern sicherstellen

Uwe Maurer, Consulting Manager Security Operations, Integralis
Insbesondere im Finanzsektor oder bei kritischen IT-Systemen ist die Aufmerksamkeit, die den Tätigkeiten von IT-Beratern entgegengebracht wird, in den letzten Jahren stark gewachsen. Die meisten Regularien behandeln das Thema Third-Party-Access besonders kritisch, trotzdem werden die möglichen Bedrohungen von externen IT-Beratern häufig unterschätzt.

In praktisch jedem Unternehmen werden IT-Berater eingesetzt, gerade bei sensiblen IT-Systemen. Sie sind oft „Business-Enabler“, und bringen neue Ideen oder Aspekte ein. Vor allem können notwendige Kompetenzen sofort eingesetzt und müssen nicht mühevoll im eigenen Unternehmen entwickelt werden. Die dafür erforderlichen Investitionen können gespart und Scaling-Effekte genutzt werden. IT-Berater verkürzen vor allem die „Time-To-Market“ und ermöglichen schnelle Änderungen im Unternehmen. Zudem bringen sie in vielfältiger Form Erfahrungen mit, die sie bei anderen Kunden erworben haben. Es liegt in der Natur der Dinge, dass externe IT-Berater vor allem bei den „interessanteren“ Systemen mit kritischen Daten tätig sind – natürlich auch in der IT-Sicherheit. Dabei darf die Informationssicherheit nicht reduziert werden. Zugriffe und Aktivitäten der externen IT-Berater müssen laufend kontrolliert werden, da ist auch der Standard ISO 27002 eindeutig .

Besondere Situation durch enge Einbindung

Externe IT-Partner arbeiten gerne in einer guten Mischung von on-site und off-site Tätigkeiten. Vielfach ist es so, dass beide Vertragspartner aufgrund der zeitlichen oder funk-

tionalen Kritikalität einen schnellen Remote-Zugang wünschen. Diese Fernwartungs-Zugänge entsprechen jedoch in vielen Fällen nicht den Erwartungen an die IT-Sicherheit. Oft sind die Zugänge gerade zu den kritischen Systemen ohne Rückfrage oder speziellen Fernwartungsauftrag freigeschaltet. Zunehmend werden asynchrone Zugangs-Verfahren eingesetzt. Dabei werden während der externen Entwicklung bereits Zugriffs-Schnittstellen über Agenten oder Services eingerichtet, die bei Bedarf aktiviert werden können.

Viele Anwendungen oder Systeme sind so komplex, dass sie nur noch von wenigen Spezialisten ausreichend verstanden werden. Sollten Funktionen für kritische Prozesse betroffen sein, wird der Anwendungssupport oft sofort und einfach benötigt. Manche IT-Berater sind als sogenannte „Residentials“ oder als „Body-Leasing“ so häufig im Unternehmen, dass sie wie interne Kollegen behandelt werden. Dabei ist allerdings die persönliche Bindung an das Kunden-Unternehmen nicht so selbstverständlich wie bei internen Mitarbeitern.

Bedrohungen durch externe IT-Berater?

IT-Berater können durchaus auch ein Bedrohungspotenzial für die



Unternehmen darstellen. Es fällt einem Spezialisten nicht schwer, einen vollständigen Ausfall von kritischen Systemen direkt oder über andere Mitarbeiter zu veranlassen. Bei langjährigen Geschäftsbeziehungen ist das Potenzial noch höher. Denn die Daten und Systeme können, absichtlich oder unabsichtlich, in einen Zustand geraten, in dem eine vollständige Abhängigkeit vom Berater entsteht.

Egal warum ein externer IT-Berater unzufrieden wird und dafür die Schuld bei seinem Arbeitgeber oder auch beim Auftraggeber sucht. Es treten immer wieder Fälle auf, bei denen ein Schaden beim wichtigsten Kunden verursacht wird, um der eigenen Firma nachhaltig zu schaden. Es gibt keine typischen Bedrohungsszenarien, diese Spezialisten sind meist in der Lage, sehr komplexe und vielstufige Angriffspfade oder langandauernde und individuelle Angriffstypen zu entwickeln und anzuwenden.

Wesentlich häufiger als eindeutige Angriffe findet man aber Verstöße gegen die Richtlinien. Insbesondere unberechtigte Kopien von Produktionsdaten für Testzwecke oder von „eigenen“ Entwicklungen zu sogenannten „Backup-Zwecken“ finden sich häufig bei einer Untersuchung. Oft ist dabei nicht klar, welche Konsequenzen solche Verstöße haben können. Auch durch falsche Beratung kann ein externer

Möglichkeit in Betracht ziehen: Externe Berater können Sicherheitsvorfälle verursachen

Consultant Schäden anrichten. In den meisten Fällen passiert dieses aber unabsichtlich.

Schäden und Bedrohungen entstehen meist durch Zeitdruck oder aufgrund von Nachlässigkeiten. In der Konsequenz gibt es aber kaum einen Unterschied zu einem gezielten Angriff auf die IT-Sicherheit. Zudem sind die externen IT-Berater oft in der Lage, sich Zugang zum Netz zu verschaffen, auch nachhaltig. Eine übergreifende Risiko-Analyse für den Einsatz von IT-Partnern ist kaum möglich, es muss fallbezogen analysiert werden.

Wie können sich Unternehmen schützen?

Das kurze Zwischenfazit könnte den Eindruck erwecken, dass Vertrauen zu externen IT-Partnern notwendig, aber effektiv nicht möglich ist. Das bedeutet aber nicht, dass es keine Mittel gibt, die Informationen auch in diesem Bereich zu schützen. Allerdings muss IT-Partner-Sicherheit vielfältigen Bedingungen genügen. Die in erster Linie gewünschten Wirkungen der höheren Flexibilität und der schneller verfügbaren Kompetenz dürfen nicht behindert werden. Ebenso wenig darf die bestehende Vertrauensbeziehung zwischen Auftraggeber und externem Berater unter IT-Sicherheitsmaßnahmen leiden. Es sind im Bereich der externen IT-Berater genug regulative Anforderungen zu berücksichtigen, beispielsweise beim Datenschutz, bei den BSI-Prüfungen und insbesondere bei ISO 27001-Audits (27002 Kapitel 6.2 „External Parties“). Anstelle einer umfassenden Liste von möglichen Compliance-Anforderungen sei hier darauf hingewiesen, dass man davon ausgehen kann, dass relevante Regularien das Thema „externe IT-Berater“ besonders kritisch behandeln.

Welche wesentlichen Elemente müsste ein Sicherheitskonzept oder Framework für IT-Partner somit haben? Nur technische oder prä-



Uwe Maurer ist CISSP und Consulting Manager Security Operations bei Integralis

ventive Maßnahmen reichen nicht aus, sie müssen um Aktivitäten auf der organisatorischen Ebene ergänzt werden. Aufklärung tut Not, man muss „Awareness“ schaffen, nicht nur im Unternehmen, sondern auch bei den Beratern. Oft sind die möglichen Konsequenzen von Fehlverhalten nicht ausreichend bekannt. Um die kritischen Daten und Systeme, mit denen IT-Partner zu tun haben, fallweise klassifizieren zu können, muss die Beschäftigung von IT-Beratern der IT-Abteilung bekannt sein. Oft ist es auch sinnvoll, sich intensiv mit dem regulativen Umfeld zu beschäftigen. Vielfach lohnt es sich, interne Sicherheitsstandards nochmals unter die Lupe zu nehmen und zu überarbeiten, beispielsweise die Fernwartungsrichtlinie aber auch Erklärungen zum Datengeheimnis etc. Noch wichtiger ist es, das Auftragswesen für die Beschäftigung von IT-Beratern zu untersuchen. Die Vertragsgestaltung sollte die Wahrung der Informationssicherheit als wesentliches Qualitätsmerkmal enthalten.

Pflichten des Beraters

Es kann vom IT-Partner erwartet werden, dass er Rücksicht auf die Interessen seines Auftraggebers nimmt und Richtlinien im Bereich

der Datenübertragung und der Zugangspunkte und Schnittstellen akzeptiert. Beispiele dafür sind Regelungen für den Anschluss von Computern an das LAN oder die Nutzung von USB-Devices. Ebenso sollten der Aufbau von Tunneln und der Zugriff auf unternehmensfremde Systeme, die Internet-Nutzung und die Sicherheit von gelieferten Systemen und Programmen geregelt werden.

Zu den organisatorischen Maßnahmen gehört auch, dass die Betriebsprozesse die Sicherheit im Bereich der Partner unterstützen. Mit einem funktionierenden System- und Change-Management ist die Komplexität des Gesamtsystems geringer und es bestehen bessere Möglichkeiten zur Überwachung. Das Ticketing-System kann ebenfalls unterstützend wirken. Fernwartungs-Arbeiten könnten beispielsweise nur mit einem gültigen Ticket mit bestimmten Zielsystemen und -objekten, Startzeit, Dauer, Zugriffssystem und definiertem Account freigegeben werden.

Zudem gibt es seit Jahren ausgezeichnete, präventive Sicherheitstechniken. Neben der klassischen Verschlüsselung von Verbindungen, E-Mails, Dateiodnern, Devices oder Platten sollte auch die Verschlüsselung in den Datenbanken geprüft werden. Für die exportierten Daten setzt sich immer mehr Digital Rights Management (DRM) durch. Allerdings ist gerade im Umgang mit IT-Partnern ohne geeignetes Key-Management und die dafür notwendigen Prozesse eine Verschlüsselung nutzlos.

Beim Account- und Berechtigungsmanagement ist vor allem im Zusammenhang mit IT-Partnern das Management der „Shared-Accounts“ kritisch. Shared Accounts sind anonyme Functional- oder Service-Accounts, die für die Funktion der Systeme benötigt werden. Beispielsweise bei Backup-Programmen oder wenn sich die Anwendung bei der Datenbank, die Datenbank beim OS oder ein Service bei einem anderen authentisiert.

Sind deren Credentials bekannt, kann man deren oft umfangreiche Rechte ohne direkte Zuordnung zu einer Person nutzen. Weil der Account oft an zahlreichen Hosts eingesetzt wird, ist es schwierig, das Passwort zu ändern. In solchen Fällen kennt ein externer Berater, selbst wenn er schon lange nicht mehr im Unternehmen ist, kritische Zugangsmöglichkeiten.

Daher werden mittlerweile solche Credentials nicht mehr einzelnen Personen mitgeteilt, sondern in sicheren Systemen verwaltet und automatisch an die betreffenden Zielsysteme und -services übergeben. So existieren klare Aufzeichnungen darüber, wer diese Aktion ausgelöst hat. Auch Application- oder Account-aware Firewalls der neuen Generation bieten sehr gute Möglichkeiten für die Aufzeichnung der Zugangszeiten und der Zugriffe selbst.

Maßnahmen nach Wichtigkeit staffeln

Die Maßnahmen sind je nach Kritikalität der geschützten Informationen einzusetzen. Beim Einsatz in kritischen Systemen, wie Leitständen oder in den Bereichen Datenbanken sowie SAP, sollten die Techniken regelmäßig überprüft werden, denn teilweise können sie gerade dort von den Spezialisten immer noch umgangen und unterlaufen werden.

Wie bei der Kontrolle von administrativen Tätigkeiten müssen insbesondere in den Bereichen, in denen IT-Partner eingesetzt werden, „detective controls“ als sinnvolle Ergänzung zu den präventiven Maßnahmen eingesetzt werden. Beim Security Monitoring kann man versuchen, durch Korrelationsregeln bekannte, unerwünschte Zustände abzubilden. Beispielsweise wird ein Alarm ausgelöst, wenn eine Fernwartungssitzung nicht genehmigt ist oder wenn andere Systeme als im Ticket ausgewiesen angesprochen werden. Die Einsatzmöglichkeiten

dieser rein regelbasierten Systeme sind allerdings gegenüber echten Spezialisten begrenzt.

In der letzten Zeit haben sich neue Entwicklungen im Bereich des Anomalie-Monitorings durchgesetzt. Sehr einfach kann man damit ungewöhnliche Parameter erkennen, bei genutzten Accounts, bei Ziel- oder Quell-Adressen oder bei den zugreifenden Systemen. Viele Sicherheitsstandards und -richtlinien lassen sich auf Host-Ebene mit sogenannten Policy-Anomalien überwachen. Dabei können für bestimmte Systeme verdächtige („suspicious“) Muster, Tools oder unerwünschte Services gemeldet werden. Oder es werden die erlaubten Services und Programme hinterlegt und jede Abweichung gemeldet. Es können Verhaltensprofile hinsichtlich Datenübertragung oder Systemzugang erstellt werden, sodass beispielsweise ein „DMZ-Jumping“ sofort gemeldet wird. IT-Partner arbeiten zudem meist auf bestimmten Zielsystemen – mit einer Aktivitätsanomalie lassen sich Abweichungen von diesen Zielsystemen erkennen.

Von Anfang an Klartext sprechen

Die Überwachung ist insbesondere in Kombination mit konkreten Richtlinien und Sicherheitsstandards ein sehr wirksames Mittel, die Vertrauensbeziehung mit den IT-Beratern auf Dauer zu fördern. Allerdings wird dringend empfohlen, die externen IT-Berater über die Überwachung in Kenntnis zu setzen und mit ihnen zu vereinbaren, wie genau bei Verstößen vorgefahren wird. In diesen Verträgen wird bestimmt, welche Notfallmaßnahmen eingeleitet werden. Dazu kann die sofortige Deaktivierung des Accounts ebenso gehören wie die Unterbrechung der Verbindung oder das Abschalten des Systems. Festgelegt sollte auch sein, wer die Folgen (und Kosten) dieser Maßnahmen bei berechtigtem Verdacht

zu tragen hat. Des Weiteren kann man als Unterstützung der Vertrauensbeziehung mit den Partnern klar festlegen, welche Kennzahlen als Orientierung für die Beachtung der Informationssicherheit des Auftraggebers genutzt werden und welche Auswirkungen eine Fehlentwicklung hat.

Zum Abschluss lässt sich Folgendes sagen: Vertrauen zu den IT-Partnern ist notwendig und normalerweise berechtigt, denn in den meisten Fällen sind die Beziehungen zwischen Kunden und ihren IT-Partnern seriös und integer. Trotzdem sollten die Möglichkeit eines, durch einen Berater verursachten Sicherheitsvorfalls diskutiert und Gegenmaßnahmen festgelegt werden. ■

ISO 27002: „The security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services. Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled.“

Schnellreferenz

IT-Grundschutzkataloge

G 2.84 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister

G 5.10 Missbrauch von Fernwartungszugängen

M 2.221 (A) Änderungsmanagement

M 2.226 (A) Regelungen für den Einsatz von Fremdpersonal

M 2.460 Geregelt Nutzung von externen Dienstleistungen

M 3.21 Sicherheitstechnische Einweisung der Telearbeiter

M 3.33 (Z) Sicherheitsüberprüfung von Mitarbeitern

M 3.44 Sensibilisierung des Managements für Informationssicherheit

M 3.50 Auswahl von Personal

M 3.55 Vertraulichkeitsvereinbarungen

M 3.83 Analyse sicherheitsrelevanter personeller Faktoren



IT-Grundschutz Wegweiser

Beratung

»Mit Sicherheit gute Geschäfte« 

Ihr Partner in Sachen IT-Sicherheit und Informationsschutz.

www.secaron.de
info@secaron.de
0811-9594-0

»IT-Sicherheit nach Maß«



secunet

Sicherheitskonzepte - Planung und Realisierung nach IT-Grundschutz

secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen
Tel.: +49 (0) 201 5454-0
E-Mail: info@secunet.com
www.secunet.com

Fachinformationen zur IT-Sicherheit

IT-Grundschutz, Awareness, Management, Recht, Datenschutz, Risikomanagement



Mehr unter:
www.viewegteubner.de

Datenschutz

TRIGONUM


consulting

Mehr Schutz durch
KOMBINIERTER SICHERHEIT

Trigonum GmbH
Notkestr. 11
22607 Hamburg
Tel.: +49 40 3199 1618 3
E-Mail: info@trigonum.de
www.trigonum.de

Identity & Access Management

bi-Cube® IAM & SSO
Identity & Access Management / Single Sign-On
www.secu-sys.de



Netzwerksicherheit

Greenbone Security Manager

IT-Grundschutz Automatisierung:

- ▶ Prüfung auf Einhaltung von Maßnahmen
- ▶ Export-Schnittstelle für Datenübernahme



Permanente Überwachung im Hintergrund:

- ▶ Alarm bei Verstoß oder Sicherheitslücke

www.greenbone.de Tel +49-541-335084-0

IBS

Prüfen mit Konzept

Your partner in compliance.
Unsere Zielsetzung ist, Ihre IT- und SAP-Systeme zu sichern, Ihre Unternehmensprozesse wirtschaftlich zu gestalten und Compliance zu gewährleisten.

Was können wir für Sie tun?

- Prüfsoftware
- Audit und Beratung
- Prüfseminare und Konferenzen
- Datenschutzprüfstelle

Simplify compliance

IBS Schreiber GmbH
040 6969 8515
info@ibs-schreiber.de
www.ibs-schreiber.de

SecuPedia

Die Plattform für Sicherheits-Informationen

Was ist eine „Digitale Signatur?“
Gleich **gratis** im Online-Lexikon der Sicherheit nachschlagen!

www.secupedia.info

Security Monitoring

P³
Consulting+Software AG
projects/products/processes

Ihr Partner im Risikomanagement
SIEM – Security Monitoring
Software/Managed Security Service

Solmsstraße 18 · 60486 Frankfurt/Main
Telefon 069-2017417-14
www.p3-consulting.de
info@p3-consulting.de

Software

BSI-Grundschutz, ISO 27001
nativ, Risikoanalyse, Audit nach ISO 19011, Datenschutz.
www.kronsoft.de

itsa Die IT-Security-Messe

16.-18. Okt. 2012, Nürnberg
Ihr bookmark für IT Security:
www.it-sa.de/newsletter

Ihre Anzeige im IT-Grundschutz Wegweiser

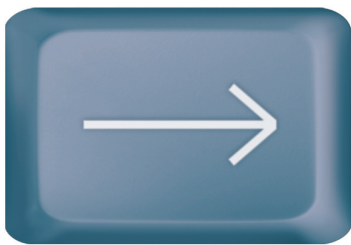
Preis s/w: 1,30 € pro mm
Preis 4c: 1,95 € pro mm
(Euroscala)
(Preis je Rubrik zzgl. MwSt.)

Ihr Kontakt zur Anzeigenabteilung

Informationsdienst
IT-Grundschutz
Birgit Eckert
Tel. +49 6725 9304-20
anzeigenleitung@secumedia.com

Ihr Kontakt zum Leserservice

Informationsdienst
IT-Grundschutz
Veronika Strauß
Tel. +49 6725 9304-27
vertrieb@secumedia.com
www.grundschutz.info



IT-Grundschatz

Informationsdienst

Hintergrundwissen und Umsetzung in der Praxis

Der Informationsdienst „IT-Grundschatz“ liefert achtmal jahrlich Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen – leicht verstandlich und praxisnah. Alle Artikel und Interviews bauen auf den Vorgaben der Grundschatzkataloge auf, sodass Sie permanent auf dem Laufenden bleiben.



Das Plus: Abonnenten erhalten gratis Zugang zum Online Heftarchiv (alle Artikel ab Ausgabe 1/2009).

News und Leseproben unter:
www.grundschatz.info

Abonnement-Bestellung Print-Abo

- Ja, ich abonniere bis auf Widerruf den Informationsdienst „IT-Grundschatz“ ab Ausgabe zum Jahresbezugspreis (8 Ausgaben, davon 2 Doppelausgaben) von 98,00 € (Inland) / 116,10 € (Ausland) inkl. MwSt. und Versandkosten (Schweiz: 187,00 SFr).
- Ich bin auch Abonnent der Zeitschrift <kes> oder WIK und erhalte daher einen vergunstigten Koppelabopreis. Koppelabopreis fur <kes> / WIK-Abonnenten: Inland 76,00 € / Ausland 84,53 € / Schweiz: 130,00 SFr (inkl. MwSt. und Versandkosten)

Abonnement-Bestellung e-Paper Abo

- Ja, ich abonniere bis auf Widerruf den Informationsdienst „IT-Grundschatz“ ab Ausgabe zum Jahresbezugspreis (acht Ausgaben) von 65,00 € inkl. MwSt. Die Zustellung der e-Paper Aboausgaben erfolgt per E-Mail als pdf bzw. Downloadmoglichkeit mit Zugangsdaten. Ich stimme der Zusendung zu.

Die SecuMedia Verlags GmbH raumt mir das Recht ein, diese Bestellung innerhalb 14 Tagen ab Bestelldatum zu widerrufen. Ich kann das Abonnement jederzeit kundigen. Zuviel bezahlte Abo-Gebuhren werden ruckerstattet. Ich bin mit der Speicherung meiner Daten einverstanden. Ich bin damit einverstanden, dass die Deutsche Post AG eine eventuell geanderte Anschrift weiterleiten kann.

Datum _____ Zeichen _____ Unterschrift _____

Bitte im Fensterumschlag oder per Fax an SecuMedia Verlags-GmbH einsenden

Fax +49 6725 5994

Absender / Firmenstempel:

SecuMedia Verlags-GmbH
Abo-Service
Postfach 12 34

55205 Ingelheim

z.Hd: _____

E-Mail: _____