



IT-SCHWACHSTELLENANALYSE

Überprüfung von IT-Systemen und Netzwerken aus Sicht eines Hackers zur Aufdeckung von Sicherheitslücken

Lieber Geschäftsleiter und IT-Verantwortliche,

wer heute IT-Systeme und Firmennetzwerke mit dem Internet verbindet, muss mit zahlreichen Gefahren rechnen, die daraus resultieren.

Durch die weltweite Verfügbarkeit der Internetanbindung, können Angriffe auf die Systeme von überall auf der Welt her erfolgen. Dabei gibt es mehrere Ziele, die von Angreifern anvisiert werden:

- Ihre Geschäftsdaten, Firmengeheimnisse und Know-How.
- Die Daten Ihrer Kunden.
- Die Ressourcen Ihrer Systeme für:
 - die Verbreitung von Spam-Mails,
 - Zwischenlager von Schadsoftware oder
 - das Ausführen von Angriffen auf weitere Systeme.
- Den Ausfall Ihrer Systeme für:
 - digitale Schutzgelderpressung oder
 - Imageschädigungen.

Die wichtigste Erkenntnis sollte für Sie jedoch sein, dass egal welche Angriffsmotive vorliegen und welche Ziele man bei Ihnen verwirklichen kann, die Tatsache entscheidend ist, dass es nur eine Frage der Zeit ist, wann Ihre IT-Systeme angegriffen werden. Selbst das noch so kleine Unternehmen wird automatisiert mittels der genutzten IP-Adressen gescannt und bei Verwundbarkeiten durch Hacker, Nachrichtendienste und Wirtschaftsspione ausgespäht und angegriffen.

Sicherheitslücken ergeben sich meist durch falsche Anwendung und Konfiguration von Schutzmaßnahmen (Faktor Mensch) oder Problemen in der verwendeten Software (Exploits, Bugs, etc.) bzw. einer Kombination beider Schwachstellen wegen der Komplexität der Systeme selbst.

Daher bieten sich regelmäßige Überprüfungen mit geeigneten Werkzeugen an, um ein Mindestmaß an Schutz zu gewährleisten und die wesentlichen Lücken aufdecken und beheben zu können.

Auch fordern die deutschen Gesetze z.B. zum Datenschutz, dem Risikomanagement für GmbHs und andere Vorschriften, einen sicheren Betrieb und regelmäßige Kontrollen, alleine schon zur Reduktion der Haftung für die Verantwortlichen im Schadensfall.

Wir bieten Ihnen daher eine professionelle und unabhängige IT-Schwachstellenanalyse an, um Ihnen die notwendigen Gegenmaßnahmen aufzuzeigen und den Angreifern zuvorzukommen. Außerdem werden diese immer häufiger von Datenschützern, Wirtschaftsprüfern, Revisoren und Versicherungen gefordert.

Carsten Knoop

Carsten Knoop
Geschäftsinhaber



Welche Risiken haben Ihre IT-Systeme?

Es gibt viele Möglichkeiten E-Mail-Server, Firewalls, Anwendungen, Datenbanken, VoIP-Systeme, Netzwerkumgebungen oder andere IT-Systeme auf mögliche Risikofaktoren zu überprüfen. Die eine Form ist ein manuelles Prüfverfahren, die andere ein (halb) automatisiertes Verfahren. Die beste Variante ist sicherlich beides zu machen, allerdings stellt sich als Unternehmer die Frage, wie man kostengünstig möglichst viele Bedrohungen aus dem Weg räumen kann.

Nicht die Frage der Firmengröße soll entscheiden, welches Verfahren Sie nutzen, sondern die Frage der wirtschaftlichsten Schutzfunktion.

Die zwei wichtigsten Entscheidungsfragen:

Sind Ihre Systeme Standard-Ausführungen ohne besondere Eigenentwicklungen oder handelt es sich um individuelle, auf Ihre eigenen Bedürfnisse angepasste oder entwickelte Software und Systeme?

Dort wo sehr viele Standardkomponenten zum Einsatz kommen, sind automatisierte und halb-automatisierte Testverfahren von außen die erste Wahl, um die wichtigsten Sicherheitslücken zu finden. Hierzu eignet sich unsere BASIC Schwachstellenanalyse am besten. Eine automatisierte Überprüfung auf bekannte Schadsoftware kann hier ergänzend eingebunden werden. Je nach Komplexität und Sicherheitsanforderungen der Systeme, ist eine zusätzliche manuelle Überprüfung von Sicherheitslücken oder sogar des gesamten Netzwerkes auch von intern ratsam. Hierbei kommt unsere PREMIUM Schwachstellenanalyse zum Einsatz.

Handelt es sich um einfache Sicherheitsvorkehrungen oder sind Sie bereits mit komplexen DMZ, WAF, IDS und anderen Sicherheitsmaßnahmen ausgerüstet und haben Ihre Systeme bereits gehärtet?

Wo besondere Sicherheitsmaßnahmen getroffen wurden bietet die BASIC Schwachstellenanalyse einen ersten Überblick über Konfigurations- und Einrichtungsfehler. Hier ist eine manuelle Prüfung als Ergänzung zu empfehlen. Hierzu eignet sich unsere PREMIUM Schwachstellenanalyse.

Außerdem gilt: je mehr sensible Daten Sie in Ihren Systemen verarbeiten und speichern, desto regelmäßiger sollte eine Schwachstellenüberprüfungen durchgeführt werden, da fast täglich neue Sicherheitslücken, Zero-Day-Exploits und andere Probleme auftauchen.

Wenn Sie unsicher sind, welches Verfahren für Sie am besten geeignet ist oder Sie noch Fragen zur Sicherheit Ihrer Systeme und Netzwerke haben, beraten wir Sie gerne.



Kontaktieren Sie uns per:

Tel.: 05221 85496-90,

E-Mail: info@audatis.de

oder nutzen Sie unser Kontaktformular auf Seite 5.

Unsere IT-Schwachstellenanalysen im Schnellüberblick

	BASIC	PREMIUM
TOP 20 Sicherheitslücken überprüfen	+++	+++
Port-Scan der Systeme	++	+++
PCI-Compliance Prüfung	++	+++
Externer Scan	++	+++
Interner Scan	+	+++
Schadsoftware Scan	+	+++
Anzahl Systemes	1 IP-Adresse	Beliebig viele IP-Adressen und Systeme
Zugriffsbereich	Nur externe Zugriffe auf das System ohne Login	Zusätzlich Überprüfungen von intern und mit Login
Beschreibung des Testverfahren	Halbautomatisiertes Testverfahren zum Überprüfen der Systeme auf die wichtigsten Schwachstellen und Sicherheitslücken durch gängige Hackermethoden	Individuelle und manuelle Testverfahren zum Überprüfen der Schwachstellen und Sicherheitslücken sowie Hackermethoden durch einen Security Experten
Abdeckung	Bietet eine gute Überprüfung mit den wichtigsten Angriffsmöglichkeiten von außen	Bietet eine sehr tiefe Überprüfung von innen und außen, die fast alle Angriffsmöglichkeiten einbezieht
Berichte	Management Summary der gefundenen Schwachstellen (in deutscher Sprache) sowie ausführlicher Bericht inkl. Beschreibung der Gegenmaßnahmen (auf Englisch)	Optional können alle Berichte auch in deutscher Sprache zur Verfügung gestellt werden
Zertifikat		
Preis	Einrichtung inkl. 1 IP-Adresse: 649,- € Weitere IP-Adressen je 69,- €	nach individuellem Angebot
Erneute/regelmäßige Prüfung	Bei gleichen IP-Adressen 20% Rabatt	nach individuellem Angebot

+ nur als Einstieg geeignet

++ gut geeignet
(Schwerpunkt: Preis-/Leistung)

+++ sehr gut geeignet
(Schwerpunkt: Höchste Sicherheit)

An
audatis[®] Consulting
Inh. Carsten Knoop
Wittekindstr. 3
32051 Herford

per Fax: 05221 85496-99
oder E-Mail: info@audatis.de

IT-Schwachstellenanalyse

- Hiermit beauftragen wir verbindlich audatis Consulting mit der Durchführung der BASIC IT- Schwachstellenanalyse und akzeptieren die AGB von audatis [Consulting](#).
- Wir möchten ein Angebot für die PREMIUM IT- Schwachstellenanalyse / Penetrationstest bekommen.
- Wir benötigen eine unverbindliche Beratung zur Auswahl der für uns passenden Analyse-Methode.

Zu prüfende IP-Adresse(n)

Gewünschter Auftragsbeginn

Auftraggeber

Firma

Straße und Hausnr.

PLZ und Ort

Telefon

Name des Vertretungsberechtigten

Datum

Unterschrift und Stempel Auftraggeber

Allgemeine Geschäftsbedingungen audatis® Consulting

I. Geltungsbereich

1. Alle unsere Angebote, Leistungen und Lieferungen erfolgen ausschließlich auf Grund dieser Geschäftsbedingungen. Spätestens mit Vertragsschluss gelten diese Bedingungen als angenommen. Sie sind unter <https://www.audatis.de/agb> einsehbar.
2. Schriftliche Individualvereinbarungen gehen diesen Geschäftsbedingungen vor.

II. Angebote

1. Abgegebene Angebote sind stets freibleibend und unverbindlich.
2. Technische und gestalterische Abweichungen von Beschreibungen und Angaben in Prospekten, Katalogen und schriftliche Unterlagen sowie Änderungen im Zuge des technischen Fortschritts bleiben vorbehalten, ohne dass hieraus Rechte gegen uns abgeleitet werden können.

III. Preise

1. Alle Preise verstehen sich ab Sitz in Herford. Entgegenstehende Vereinbarungen müssen schriftlich bestätigt werden.
2. Preisangaben, die sich erkennbar ausschließlich an gewerbliche Kunden richten, verstehen sich im Zweifel zzgl. der gesetzlichen Mehrwertsteuer.

IV. Leistungszeiten

1. Leistungsverzögerungen aufgrund von höherer Gewalt und/oder aufgrund von Ereignissen, die uns die Leistung wesentlich erschweren oder unmöglich machen, z. B. Betriebsstörungen, Streik, behördliche Anordnungen etc. berechtigen uns, die Lieferung um die Dauer der Behinderung zuzüglich einer angemessenen Anlaufzeit hinauszuschieben oder wegen des noch nicht erfüllten Teiles ganz oder teilweise vom Vertrag zurückzutreten.
2. Im Übrigen kommen wir erst dann in Verzug, wenn uns der Kunde schriftlich eine Nachfrist von mindestens einem Monat gesetzt hat. Im Falle des Verzuges hat der Kunde Anspruch auf eine Verzugsentschädigung in Höhe von 0,5% für jede vollendete Woche des Verzuges, insgesamt jedoch max. bis zu 5% des Rechnungswertes der vom Verzug betroffenen Leistungen. Darüber hinaus sind Ansprüche, insbesondere Schadensersatzansprüche jedweder Art, ausgeschlossen.
3. Sollten auf Wunsch des Kunden reservierte Arbeitstage weniger als 5 Tage vor deren Beginn durch den Kunden storniert oder verschoben werden, berechnen wir eine Ausfallgebühr i. H. von 50% der Dienstleistungssumme. Bei einer Stornierung weniger als 2 Tage vorher berechnen wir 100% der Dienstleistungssumme. Dem Kunden bleibt vorbehalten, nachzuweisen, dass der Ausfall zu keinem oder zu einem wesentlich niedrigeren Schaden geführt hat, als diese Pauschale.

V. Gewährleistung und Haftung

1. Die Gewährleistung beträgt 24 Monate.
2. Der Kunde verpflichtet sich, für die Durchführung von z.B. Schwachstellenanalyse Systeme zur Verfügung zu stellen, die nicht produktiv eingesetzt werden und bei deren Überprüfung keine Teile des Unternehmensnetzwerks in Mitleidenschaft gezogen werden können. Falls der Kunde Tests auf Systemen wünscht, die vom Kunden betrieblich verwendet werden, ist audatis Consulting vom Kunden darauf schriftlich hinzuweisen und eine Einverständniserklärung der Geschäftsleitung des Kunden vorzulegen.
3. Die für die Tests eingesetzte Software wird von audatis Consulting je nach Umfang der gewünschten Tests vorgeschlagen und ausgewählt. audatis Consulting haftet nicht für Mängel der Software Dritter.
4. In jedem Fall wird der Kunde darauf hingewiesen, dass eine Schwachstellenanalyse den Ausfall einzelner oder aller Systeme des mit dem überprüften Rechner verbundenen Netzwerks zur Folge haben kann sowie ggf. einer oder mehrere Rechner des Netzwerks neu installiert werden müssen. Auch wenn keine sogenannten kritischen Tests durchgeführt werden, kann aufgrund von Fehlfunktionen der angreifenden oder angegriffenen Software nicht ausgeschlossen werden, dass einzelne Rechner oder Netzwerkkomponenten ausfallen. Daher wird jegliche Haftung, insbesondere wegen Verlust der Vertraulichkeit, der Verfügbarkeit oder der Integrität von Daten oder daraus erwachsenden Folgeschäden ausgeschlossen.

5. Für Schäden wegen Rechtsmängeln und Fehlens zugesicherter Eigenschaften haften wir unbeschränkt. Die Haftung für anfängliches Unvermögen, Verzug und Unmöglichkeit wird auf solche Schäden begrenzt, mit denen vernünftiger Weise zu rechnen ist, die Haftung pro Schaden beträgt jedoch maximal 250.000,- EUR.
6. Im Übrigen haften wir unbeschränkt nur für Vorsatz und grobe Fahrlässigkeit auch unserer gesetzlichen Vertreter. Für das Verschulden sonstiger Erfüllungsgehilfen haften wir nur im Umfang der Haftung für anfängliches Unvermögen nach dem voranstehenden Absatz.
7. Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrenstprechender Anfertigung von Sicherungskopien von Daten und Programmen (einschließlich des Betriebssystems) auf einem geeigneten Backupmedium eingetreten wäre.
8. Sämtliche Ansprüche, die sich gegen uns richten, sind ohne unsere schriftliche Zustimmung nicht abtretbar und können ausschließlich vom Kunden selbst geltend gemacht werden.

VI. Zahlung

1. Soweit nicht anders vereinbart ist, sind unsere Rechnungen ohne Abzug sofort zur Zahlung fällig.
2. Wir sind berechtigt, trotz anderslautender Bestimmungen des Kunden Zahlungen zunächst auf dessen ältere Schuld anzurechnen.
3. Gerät der Kunde in Verzug, so sind wir berechtigt, von dem betreffenden Zeitpunkt ab Zinsen in banküblicher Höhe, mindestens jedoch in Höhe von 8%, zu berechnen.
4. Kommt der Kunde seinen Zahlungsverpflichtungen nicht vertragsgemäß nach, stellt er seine Zahlungen ein oder werden uns andere Umstände bekannt, die die Kreditwürdigkeit des Kunden in Frage stellen, so sind wir berechtigt, die gesamte Restschuld fällig zu stellen, Vorauszahlungen oder Sicherheitsleistungen zu verlangen und die Forderungen zu verkaufen.
5. Der Kunde ist zur Aufrechnung, Zurückbehaltung oder Minderung, auch wenn Mängelrügen oder Gegenansprüche geltend gemacht werden, nur berechtigt, wenn wir ausdrücklich zustimmen oder wenn Gegenansprüche rechtskräftig festgestellt sind.

VII. Dienstleistungen

1. Projekte können nur nach Maßgabe des Vertrags auf das Ende des jeweiligen Projektabschnittes nach der Leistungsbeschreibung gekündigt werden.
2. Vertragsinhalt wird nur der zu Beginn des Projektes schriftlich festhaltene Leistungsumfang. Vertragsänderungen sind nur mit schriftlicher Bestätigung des Auftragnehmers möglich. Der Auftragnehmer ist nicht zu wesentlichen Vertragsänderungen verpflichtet. Der Auftraggeber verpflichtet sich, bei Vertragsänderungen vereinbarte Fristen angemessen zu verlängern.

VIII. Lizenz-, Schutz- und Urheberrechte

Software, die wir auf Wunsch des Kunden auf Systemen des Kunden installieren sollen, muss vom Kunden gestellt werden. Der Kunde hat dafür zu sorgen, dass die benötigte Anzahl von Softwarelizenzen gemäß den Bestimmungen des Urheberrechts zur Verfügung gestellt werden.

IX. Erfüllungsort und Gerichtsstand

1. Erfüllungsort von Lieferungen und Leistungen ist Herford.
2. Es wird ausschließlich Herford als Gerichtsstand vereinbart, soweit die §§ 38, 40 ZPO nicht entgegenstehen.
3. Es gilt ausschließlich das Recht der Bundesrepublik Deutschland.

X. Schlussbestimmungen

Sollten einzelne Bestimmungen nichtig, unwirksam oder anfechtbar sein oder werden, sind sie so auszulegen bzw. zu ergänzen, dass der beabsichtigte wirtschaftliche Zweck in rechtlich zulässiger Weise möglichst genau erreicht wird; die übrigen Bestimmungen bleiben davon unberührt. Sinngemäß gilt dies auch für ergänzungsbedürftige Lücken.



Weitere Büros

Berlin-Brandenburg (Potsdam)
Rhein-Main-Neckar (Birkenau)
Rhein-Ruhr (Köln)

Hauptsitz/Büro Ostwestfalen

Wittekindstr. 3 | 32051 Herford
Fon: 05221 85496-90
Fax: 05221 85496-99
E-Mail: info@audatis.de
Internet: www.audatis.de