Positionspapier SIEM

ISACA Germany Chapter

Vorschlag für einen Protokollierungsstandard mit dem Ziel einer Eventerkennung, die einfach in der Umsetzung ist und gleichzeitig Aufwände reduziert.

Security ist wichtiger denn je, jedoch für Unternehmen aufwändig und komplex in der Umsetzung. Insbesondere das Security Monitoring verursacht hohe Aufwände und erfordert oftmals nicht vorhandenes Personal. Wir stellen einen Ansatz vor, der die ursächlichen Probleme adressiert und beschreibt, wie Security Monitoring in der Breite ermöglicht werden kann.

Einleitung

Damit wir die verbundenen Themen der Protokollierung und Eventerkennung besser verstehen, beginnen wir zunächst mit einer Heranführung. Wir leben in einer hochentwickelten Gesellschaft: Autos sind für fast jeden erschwinglich. Smartphones erlauben es uns nicht nur, mit anderen zu telefonieren, sondern über das Internet Musik zu hören, Filme zu sehen oder unseren Alltag zu planen. Kühlschränke, Fernseher, Mikrowellen, Waschmaschinen, Energie- und Wasserversorgung oder auch so einfache allgegenwärtige Gegenstände wie LED-Leuchtmittel, Kugelschreiber oder Plastikflaschen... Selbst mit Anleitung würden Menschen des Mittelalters für das Schaffen der zivilisatorischen und industriellen Voraussetzungen zur Herstellung Vergleichbares viele Jahre brauchen und noch länger, bis sie dieses in Masse reproduzieren könnten.

Insbesondere die Fähigkeit der Massenproduktion ist die grundlegende Basis für unser modernes Leben. Wie würden unsere Lieferketten ohne Möglichkeiten zur Kühlung aussehen? Wie lange könnten die Menschen am Tag arbeiten, wenn kein elektrisches Licht gesichert zur Verfügung stünde?

Der heutige Zustand ist das Ergebnis einer langen Folge von Entwicklungen. Diese und viele weitere gehen immer schneller voran. Ein wichtiger Treiber hiervon ist die Normung bzw. Standardisierung, die uns viele Vorteile gebracht hat, insbesondere:

#	Vorteile der Normung
1	Komponenten oder Ersatzteile können von vielen unterschiedlichen Herstellern produziert und austauschbar eingesetzt werden.
2	Einheitliche Qualitätsstandards und Kontrollen werden möglich.
3	Kosten und Entwicklungszeit sinken, insbesondere durch Skaleneffekte.
4	Es entstehen abgegrenzte Themenfelder, auf die sich Fachleute konzentrieren und diese effizient weiterentwickeln können, ohne dass der Bezug zum übergeordneten Themenfeld verloren geht.

Tabelle 1: Vorteile der Normung

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Der Beginn der Geschichte der Normung geht bereits länger zurück, insbesondere wenn man historische Normen einbezieht. Die erste Norm in Deutschland wurde 1918 mit der DIN 1 für die Maße von Kegelstiften veröffentlicht. Es folgten bis heute zahlreiche weitere Normen wie bspw. 1922 die DIN 476, die u.a. das bekannte DIN A4 Format für Papier festlegt.

Die Herausforderungen für Unternehmen

In der Informationstechnologie (IT) ist diese Entwicklung bisher nur in Teilen angekommen. Überwiegend konzentriert sich Normung hier auf Hardware wie USB-Standards oder Platinen. Bis auf einige Teilbereiche wie bspw. Internetprotokolle und Grafikformate gibt es vielmehr Richtlinien oder Best Practices als Normungen. Will man Software miteinander kombinieren, stößt man schnell auf zahlreiche Probleme:

#	Probleme bei der Kombination von Software
1	Formate müssen umgewandelt werden, und es gibt keine einsehbare öffentliche Dokumentation oder auch Garantie, dass sich das Format mit der nächsten Version nicht ändert.
2	Werden standardisierte Formate unterstützt, dann oft nicht mit dem vollen erforderlichen Funktionsumfang oder Detailgrad.
3	Teilweise wird von Herstellern bewusst das Zusammenspiel ihrer eigenen mit anderer Software erschwert, weil sie sich davon einen Wettbewerbsvorteil versprechen.
4	Einhaltung rechtlicher Vorgaben insbesondere aus DSGVO, Geschäftsgeheimnisgesetz, HGB & AO etc.

Tabelle 2: Probleme bei der Kombination von Software

Dies macht es für Unternehmen[1] schwierig, ihre geschäftlichen und betrieblichen Anforderungen miteinander zu vereinbaren: Nehmen sie möglichst wenige, vielleicht nur einen Hersteller, passt alles meist gut zusammen – allerdings sind sie von diesen abhängig. Nimmt man unterschiedliche Hersteller, sind die Lösungen vielleicht punktuell besser, jedoch im Normalfall inkompatibel. Wiederum alles selbst machen bedeutet: einen Stab von qualifizierten Mitarbeitern zu unterschiedlichen Themen aufzubauen und zu halten und nicht schnell durch den Erwerb von Standardprodukten auf Änderungen reagieren zu können. Die meisten entscheiden sich daher für eine Kombination dieser beiden Ansätze, was die Probleme zwar mindert, aber nicht löst.

In kaum einem Bereich der IT wird dies so deutlich wie beim Security Monitoring, also der fortlaufenden Überwachung der Sicherheit von IT-Systemen. Dies ergibt sich zunächst aus dem Umfeld:

#	Schwieriges Umfeld für Unternehmen
1	Unternehmen haben oft zahlreiche unterschiedliche Produkte im Einsatz: Firewalls, Anti-Virenscanner, Mailserver, Router/Switches, Server, Endgeräte (Notebooks, Handys, …), Berechtigungsmanagementsysteme, Webserver, geschäftsspezifische Anwendungen... Für alle diese und noch weitere gibt es nicht nur zahlreiche unterschiedliche Hersteller, sondern auch regelmäßig Veränderungen durch neue Versionen
2	Die Bereiche, in denen IT Einzug hält, werden ständig mehr und die Systeme komplexer und abhängiger voneinander

[1] auch Behörden, der Fokus liegt bei diesem Positionspapier aber allerdings auf der Wirtschaft

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

3	Kleinere Unternehmen haben oft wenig bis kein Fachpersonal, das sich mit der Breite der Produkte ausreichend auskennt
4	Mittlere oder größere Unternehmen lagern häufig Aufgaben an Dienstleister aus. So betreibt dann bspw. ein Dienstleister die Firewalls und 80% der Server, ein weiterer 20% der Server sowie die Clients und die Endgeräte, und ein oder mehrere weitere die Netzwerkinfrastruktur sowie die anderen Produkte und Lösungen
5	Aufgrund der zahlreichen unterschiedlichen Produkte muss sich das Fachpersonal mit all diesen entweder eingehend beschäftigen (Zeit), oder kann sich nur auf wenige in der ausreichenden Tiefe konzentrieren (Scope)
6	Gesetze, Regularien, Vorschriften und geo- oder sicherheitspolitische Faktoren schränken die Auswahl der nutzbaren Produktpalette ein oder reduzieren diese auch nach einer erfolgreichen Einführung
7	Angriffe auf die IT von Unternehmen, insbes. Cyberattacken, werden zu einer immer größeren Bedrohung und werden lt. Untersuchungen inzwischen als größtes Geschäftsrisiko angesehen[2]

Tabelle 3: Schwieriges Umfeld für Unternehmen

Dieses Umfeld ist ohne Zweifel komplex. Doch in Bezug auf Security Monitoring wird es noch weiter erschwert, da es hier keine verbindlichen oder zumindest ausreichend unterstützte Normen gibt, wie für die Überwachung erforderliche Daten erhoben, gespeichert, kommuniziert und ausgewertet werden sollen. Bei einer Veränderung der Softwarelandschaft, z.B. Einbringen neuer Software, Abschaffung oder Veränderung bisheriger Software, muss diese stets geprüft und das Security Monitoring angepasst werden.

Heute: Zahlreiche unterschiedliche Logformate, die z. T schon verarbeitet wurden:

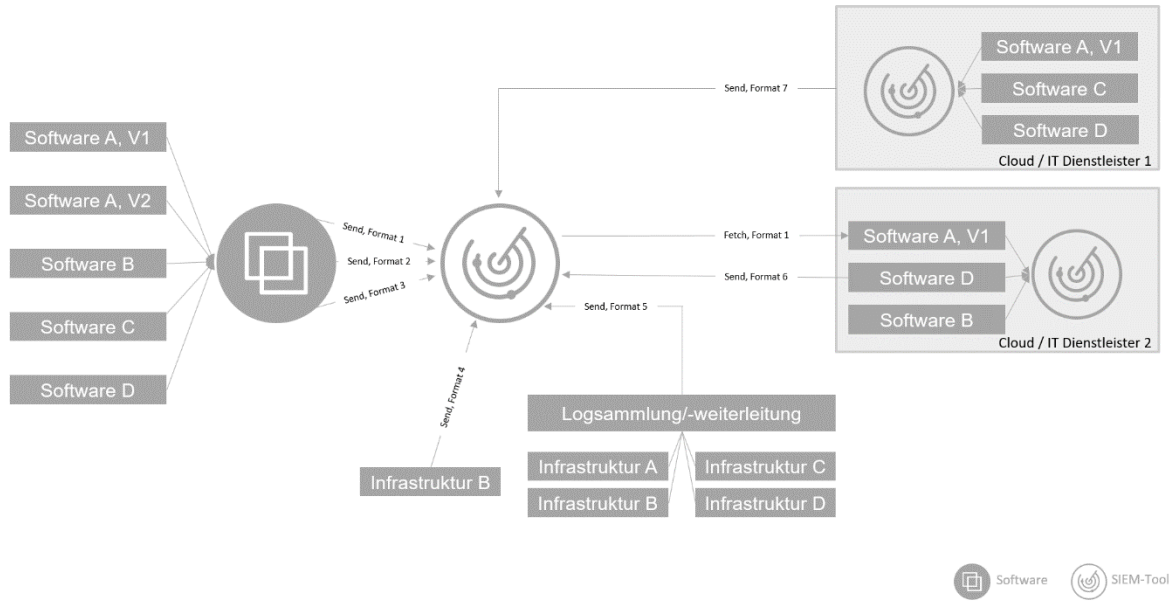

Abbildung 1: Unterschiedliche Logformate

[2] Allianz Risikobarometer: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html

Hierbei fällt dann besonders zur Last, dass sich damit beauftragte Mitarbeitende nicht nur mit einer Thematik und einer Software auskennen müssen. Vielmehr müssen sie Kombinationen von Software (Firewall A mit Syslog-Server-Variante B), Kommunikationsprotokollen (bisher sftp, neu https außer im Fall x), Übertragungswegen (ver-/unverschlüsselt, Netzwerk/Datei, innerhalb/außerhalb Firmennetzwerk), rechtliche Vorgaben (für die Kommunikation von Software A mit Software B muss Eigenschaft x aktiviert werden, das zeichnet aber Daten auf, die nach europäischem Datenschutzrecht nicht zulässig sind) und mehr beachten (vgl. auch Tabelle 2).

Aufgrund der Breite und Tiefe dieser Anforderung ist es nicht zu erwarten, dass mittels weniger Mitarbeitenden alles erforderliche Wissen vorhanden ist. Dies bedeutet Einarbeitung und/oder zusätzlich das Hinzuziehen externer Expertise. Das wiederum bedeutet Zeitverlust und Aufwand, so dass erhöhte Kosten auf Unternehmen zukommen. Oftmals müssen dann Risikobetrachtungen durchgeführt und geschäftliche Entscheidungen dahingehend getroffen werden, ob die Verzögerungen und Kosten leistbar sind. Auch müssen Verhandlungen mit Dienstleistern und anderen Vertragspartnern durchgeführt werden, um bestehende Leistungserbringungen auszuweiten oder neue hinzuzufügen.

Die Kosten für adäquate Security, insbesondere im Fall von Security Monitoring, werden stetig mehr. Dies führt dann auch zu einem weiteren typischen Problem: Security wird als Störfaktor und Kostentreiber anstelle als “Enabler” gesehen, denn all diese Aktivitäten sind diametral zu schnellen, unkomplizierten, betrieblichen und geschäftlichen Veränderungen, die für Unternehmen in einer wettbewerbsorientierten Welt wesentlich sind.

Wird es also immer komplizierter und teurer? Benötigen Veränderungen in einem Unternehmen immer mehr Vorlauf und Experten? Oder gibt es eine andere Lösung?

Die Idee: Von der Einzelfertigung zur Massenproduktion

Es gibt eine Lösung: 100 Jahre nach der DIN-Normierung für Papier normieren wir das Security Monitoring. Anstelle einer stets individuellen Einzelfertigung von Protokollen tritt die Massenproduktion von einheitlichen Logs. Für logbasierte Überwachung bedeutet dies: Anstelle stets für jede Technologie – ob Betriebssystem, Router, Anwendungen oder weiteres – individualisierte Logformate einzusetzen, die wiederum individualisierte Konvertierer/Übersetzer (“Parser”) und Implementierungen in Überwachungslösungen erfordern, wird ein einheitlicher Standard geschaffen:

Komponenten der Norm	Beschreibung
Erhebung: Spezifizierte Erfassung	Was in welchem Detailgrad von welcher Art von Software aufgezeichnet werden soll.
Speicherung: Spezifiziertes Logformat	Wie es aufgezeichnet werden soll – Formate, Kodierung, Inhalte, Integrität etc.
Kommunikation: Spezifizierte Übertragungsmechanismen	Wie die Logs zum Auswertungsort gelangen.
Integration: komplexe Unternehmensstrukturen	Wie Logs bei Auslagerungen dennoch einheitlich von Dienstleistern bereitgestellt werden können.
Auswertung: Standardisierte Use Cases	Einheitliche Regelwerke, die auf Basis der standardisierten Logs ausgewertet werden können.
Rahmen: Erfüllung von gesetzlichen und regulatorischen Anforderungen und Best Practices	Beachtung bei der Spezifikation der Norm.

Tabelle 4: Komponenten der Norm

Zentrale Ziele dieser Norm wären:

Nutzen der Norm	Beschreibung
Kosteneinsparungen	Geringere Vorlaufzeiten und Anpassungsbedarf bei Veränderungen der Softwarelandschaft; Weniger Kombinationen von Produkten und somit weniger breit und gleichzeitig tief aufgestelltes Personal erforderlich; Weniger Einzelbetrachtung und Individualisierung von Lösungen, bspw. bei Integration von Dienstleister-Systemen; Für viele kleine und mittelständische Unternehmen wird hierüber Security Monitoring bezahlbar.
Skalierende Sicherheit	Hersteller und Dienstleister können parallel arbeiten und sicherstellen, dass sie auch mit neuen Produktversionen die Norm einhalten.
Fokussierung auf Nutzung der Daten	Security Experten können sich auf die Daten und somit auf die Sicherheit konzentrieren, nicht auf die Integration.
Reduktion Komplexität	Weniger schwierige Produktkombinationen, nur wenige Integrationsschemata erforderlich. Zusätzlich sind Protokollinformationen in einem einheitlichen Format und erfordern daher weniger spezialisiertes Knowhow bei Analysten. Das vereinfacht und beschleunigt die Auswertung und steigert die Qualität der Analysen.
Standarisierte Tools und Services möglich	Hersteller von Überwachungssoftware wie SIEM-Lösungen können standardisierte Parser und Regelwerke zur Verfügung stellen; Dienstleister können basierend auf der Norm standardisierte Überwachungsdienstleistungen (bspw. SOC - Security Operating Center) anbieten und sich über Standard- und zusätzliche Leistungen differenzieren
Flexibilität und Wettbewerb	Die Norm sollte ein Qualitätsmerkmal (Siegel) werden, so dass Unternehmen dieses erfüllen müssen, um im Wettbewerb zu bestehen. Eine regelmäßige Weiterentwicklung der Norm zur Anpassung an technische Neuerungen und neue Anforderungen soll die erforderliche Flexibilität gewährleisten.
Verbesserung des Marktangebots an Security Experten	Das Feld für Security Monitoring wird differenzierter und übersichtlicher, so dass Spezialisierungen auf die eigentliche Kernaufgabe – die Überwachung – besser möglich werden. Es ist zu erwarten, dass dies auch die Hürde für den Einstieg senkt.
Unterstützung Geschäftsziele	Security Monitoring als Teil der IT Security wird planbarer, greifbarer und Widersprüche zwischen geschäftlichen Anforderungen und Security-Anforderungen werden reduziert.
Abwehr wirtschaftlicher Schäden	Durch die Normierung wird eine schnellere Anbindung von Lösungen möglich. Somit können Angriffe schneller erkannt und abgewehrt werden.

Tabelle 5: Nutzen der Norm

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Am Beispiel der o. a. Architektur zeigen sich die Vorteile nach der Umsetzung:

Normiert: Einheitliches Format

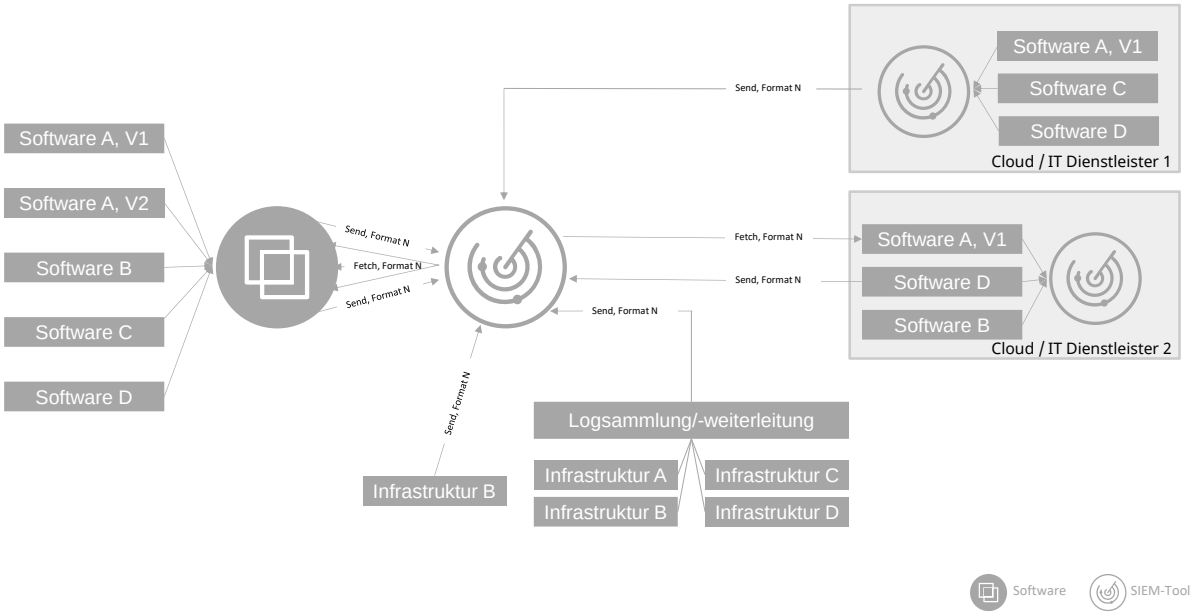

Abbildung 2: Einheitliches Format

- Es gibt nur noch ein Format anstatt mind. acht plus Varianten. Die Aufwände für Kontrollen auf Anpassungsbedarf, Anpassungen und (Regressions-) Testing sind stark vermindert oder entfallen.
- Der Integrationsmechanismus, der sich je nach Anbindungsart unterscheidet (direkt, indirekt via. Logsammlung selbst oder durch Clouds und IT-Dienstleister), ist einheitlich. Gerade bei der Integration weiterer IT-Dienstleister sowie Clouds oder bei Wechseln vereinfacht dies nicht nur die Technologie, sondern auch Verhandlungen (Implementierungsszenarien, was kann ein Dienstleister anbieten etc.).

Wir empfehlen daher die Erarbeitung der Punkte in Tabelle 4 und eine entsprechende Umsetzung in eine Norm. Diese würde aus einem Kern und flexiblen Erweiterungen bestehen:

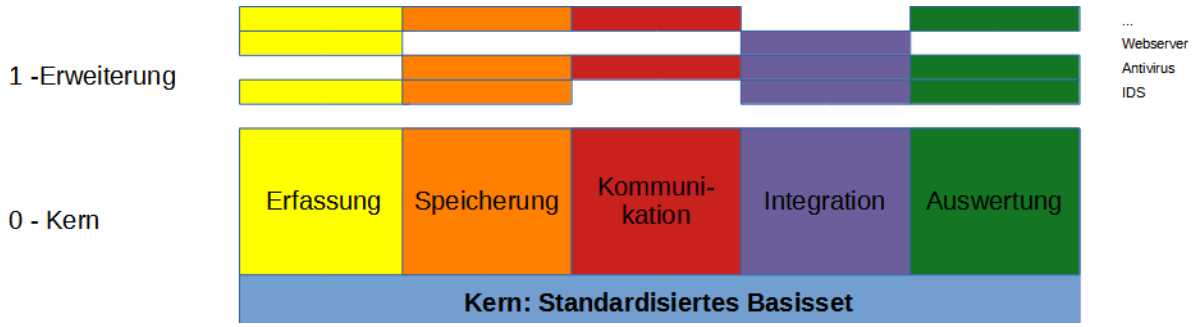

Abbildung 3: Standardisiertes Basisset

- Der Kern wäre ein Basis-Set, dass das grundlegende Minimum an Ereignissen inkl. Feldern, Inhalten, Speichermechanismen etc. festlegt. Dazu gehören auch definierte Mechanismen für Softwarehersteller, zusätzliche Informationen abzulegen.

- Die Erweiterungen würden für unterschiedliche Technologien zusätzliche Felder, Inhalte etc. definieren. Bspw. muss ein „Intrusion Detection System“ (IDS) andere Informationen als ein „Network Access Control“ (NAC) System speichern können. Sollten diese Informationen zu spezifisch sein, um ins Basis-Set aufgenommen werden zu können, so gehören sie in die Erweiterung.

Damit die Norm Wirkung entfalten kann, muss sie verschiedene Anforderungen erfüllen:

Anforderungen an die Norm	Beschreibung
Verbindlichkeit	Die Norm darf keinen empfehlenden, sondern muss einen verbindlichen Charakter haben.
Eignung	Die Umsetzung der Norm darf nicht zu komplex sein, sie muss einen effektiven Einsatz ermöglichen.
Weiterentwicklung	Um die wachsenden Security-Anforderungen und die fortlaufende Entwicklung neuer Technologien zu unterstützen, muss die Norm regelmäßig aktualisiert werden.
Eindeutige Versionierung[3]	Ein eindeutiges Versionsschema ist erforderlich, um Anforderungen seitens Unternehmen und seitens der Hersteller die Compliance ihrer Software ohne Missverständnisse zusammenbringen zu können.
Kostenneutral	Für eine Adaption der Norm muss ihre Spezifikation kostenfrei erhältlich sein.

Tabelle 6: Anforderungen an die Norm

Wie kann die Erarbeitung der Norm aussehen?

Wir sehen als Ziel dieses Papiers, die Zielgruppe bestehend aus Software- und Hardwarehersteller wie auch Branchenverbände und Normierungsorganisationen und -institutionen zu motivieren, zusammen einen einheitlichen Standard für Protokollierung zur Vereinfachung des Security Monitoring zu erarbeiten und zu verbreiten. Insbesondere kann so die Möglichkeit geschaffen werden, dass auch kleinere und mittelgroße Unternehmen das notwendige Sicherheitsmonitoring finanziell erschwinglich umsetzen können.

Möchten Sie zu diesem Positionspapier mit uns Kontakt aufnehmen. Dann schreiben Sie uns bitte an: FG-cybersecurity@isaca.de

Interessieren Sie sich für weitere Veröffentlichungen des ISACA Germany Chapter? Dann besuchen Sie uns jetzt auf: https://www.isaca.de/de/veroeffentlichungen-des-isaca-germany-chapters

[3] Idealerweise könnten Unternehmen und Behörden künftig beim Einkaufsprozess für Software vorschreiben, dass diese Norm Stand „2024/2“ (Beispiel) entsprechen müsse und die aktuelle Norm mit spätestens einem Jahr Verzug erfüllen müssten. Softwarehersteller, die nur „2023/1“ erfüllen, wären somit ausgeschlossen und ein einheitlicher Standard gewährleistet.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de