# Cybersecurity -

## optimieren Sie Ihre Schutzmaßnahmen

# Cybersicherheit

## Zehn bewährte Methoden

für ein sicheres Netzwerk

AXIS COMMUNICATIONS

# Einführung

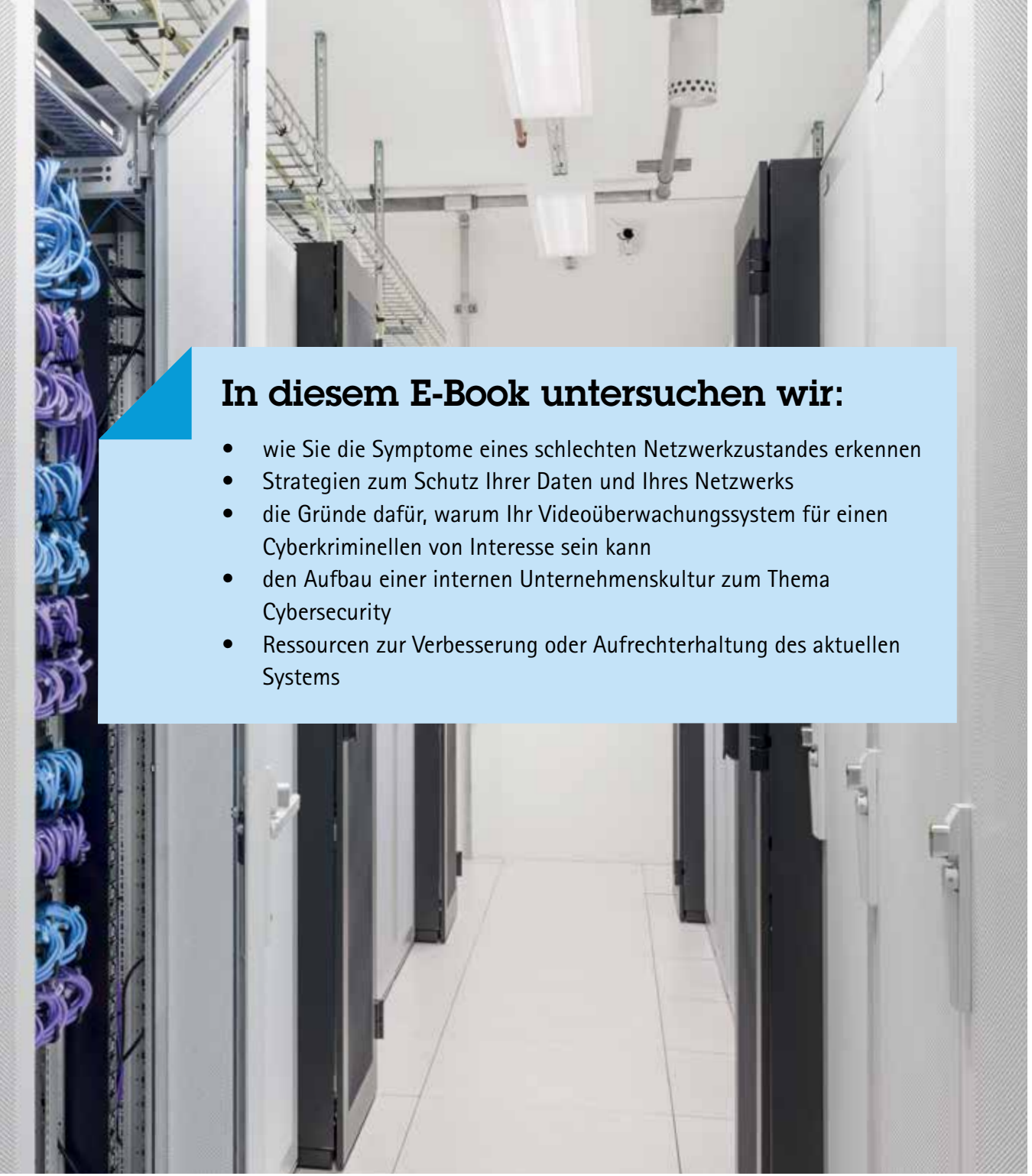
Das Thema Cybersicherheit ist in aller Munde - kein Wunder angesichts der häufigen Erwähnung in den Medien. Die Gefahren aus dem Internet, denen Unternehmen ausgesetzt sind, bewegen sich auf Rekordniveau. Die Häufigkeit von Vorfällen und deren Intensität steigt sprunghaft an.

Neuere Statistiken belegen, dass viele Organisationen nicht in der Lage sind, angemessen auf vorhandene oder neu entstehende Bedrohungen zu reagieren. Zwei von drei CIOs und CISOs geben an, dass Cybersicherheit in ihren Organisationen keine Priorität hat.* Die gute Nachricht lautet: Sie können die meisten Angriffe stoppen, wenn Sie die Schwachstellen im Netzwerk kennen und einen Plan zur Begrenzung Ihrer Anfälligkeit erstellen und umsetzen.

Hat Ihre Organisation eine effiziente Planung für die Informationssicherheit? Verfügen Sie im Fall einer Sicherheitsverletzung über eine Strategie zur Reaktion auf Cybersicherheits-Ereignisse? Haben Sie Ihr Personal aktiv zu Ihrer Cybersicherheits-Richtlinie geschult?

Die Fähigkeit, Schwachstellen zu erkennen und einen guten Zustand des Netzwerks zu gewährleisten, sind wichtige Aspekte des Risikomanagments im Netz. Doch es kann sehr schwierig sein, Ihr Netzwerk wirklich vor Bedrohungen zu schützen und gleichzeitig den Berechtigten weiterhin Zugang zu gewähren. Daher ist es wichtig, die Symptome eines schlechten Netzwerkzustandes zu erkennen und proaktiv die Sicherheit Ihres Netzwerks zu verbessern.

* 2015 Global Megatrends in Cybersecurity Ponemon Institute LLC – durchgeführt für Raytheon



## In diesem E-Book untersuchen wir:

- wie Sie die Symptome eines schlechten Netzwerkzustandes erkennen
- Strategien zum Schutz Ihrer Daten und Ihres Netzwerks
- die Gründe dafür, warum Ihr Videoüberwachungssystem für einen Cyberkriminellen von Interesse sein kann
- den Aufbau einer internen Unternehmenskultur zum Thema Cybersecurity
- Ressourcen zur Verbesserung oder Aufrechterhaltung des aktuellen Systems

Wie die physische Sicherheit ist auch eine effektive Cybersicherheit ein kontinuierlicher Kreislauf - bestehend aus der Erkennung von Schwachstellen, der Bewertung von Bedrohungen sowie der Implementierung geeigneter Maßnahmen. Die Notwendigkeit einer starken Netzwerksicherheit wird jeden Tag offensichtlicher. Um einen starken Schutz zu gewährleisten, sollten Sie nicht nur für Ihr Netzwerk, sondern für alle daran angeschlossenen Geräte das Hardening-Verfahren durchführen. So minimieren Sie Risiken, ausgehend von Schwachstellen. Verfügt Ihr Netzwerk über optimale Sicherheit?

# Symptome eines schlechten Netzwerkzustands

Ein Unternehmen ist gut gerüstet, wenn es über ein starkes und sicheres Netzwerk verfügt, Richtlinien und Prozesse eingehalten werden und alle Personen Bedrohungen aus dem Internet proaktiv begegnen und entsprechend der formulierten Ziele hinsichtlich Cybersicherheit darauf reagieren. Alle anderen Unternehmen sollten angesichts der Fokussierung auf die Cybersicherheit und der steigenden Risiken geeignete Maßnahmen ergreifen, um nicht auf dem wortwörtlichen Schleudersitz zu landen.

Ein Netzwerk mit einer schlecht implementierten Sicherheit ist für Hacker sehr attraktiv. In vielen Fällen kommt es zu einer schnelleren Verbreitung von Viren, Malware und anderen Cyber-Bedrohungen. Doch bei der großen Anzahl an aktiven Benutzern Ihres Netzwerks kann es schwer sein, ein hohes Sicherheitsniveau aufrecht zu erhalten, ohne die Produktivität zu beeinträchtigen.

Sind Sie und Ihr Netzwerk auf einen Angriff vorbereitet? Sie werden nun einige Methoden kennenlernen, um zu erkennen, ob der Zustand Ihres Netzwerks einer Verbesserung bedarf. Nach der Analyse und Bewertung können Sie Korrekturen an Ihren Richtlinien und Verfahren vornehmen, um einen geschlossenen Cybersecurity-Plan zu erstellen.

1

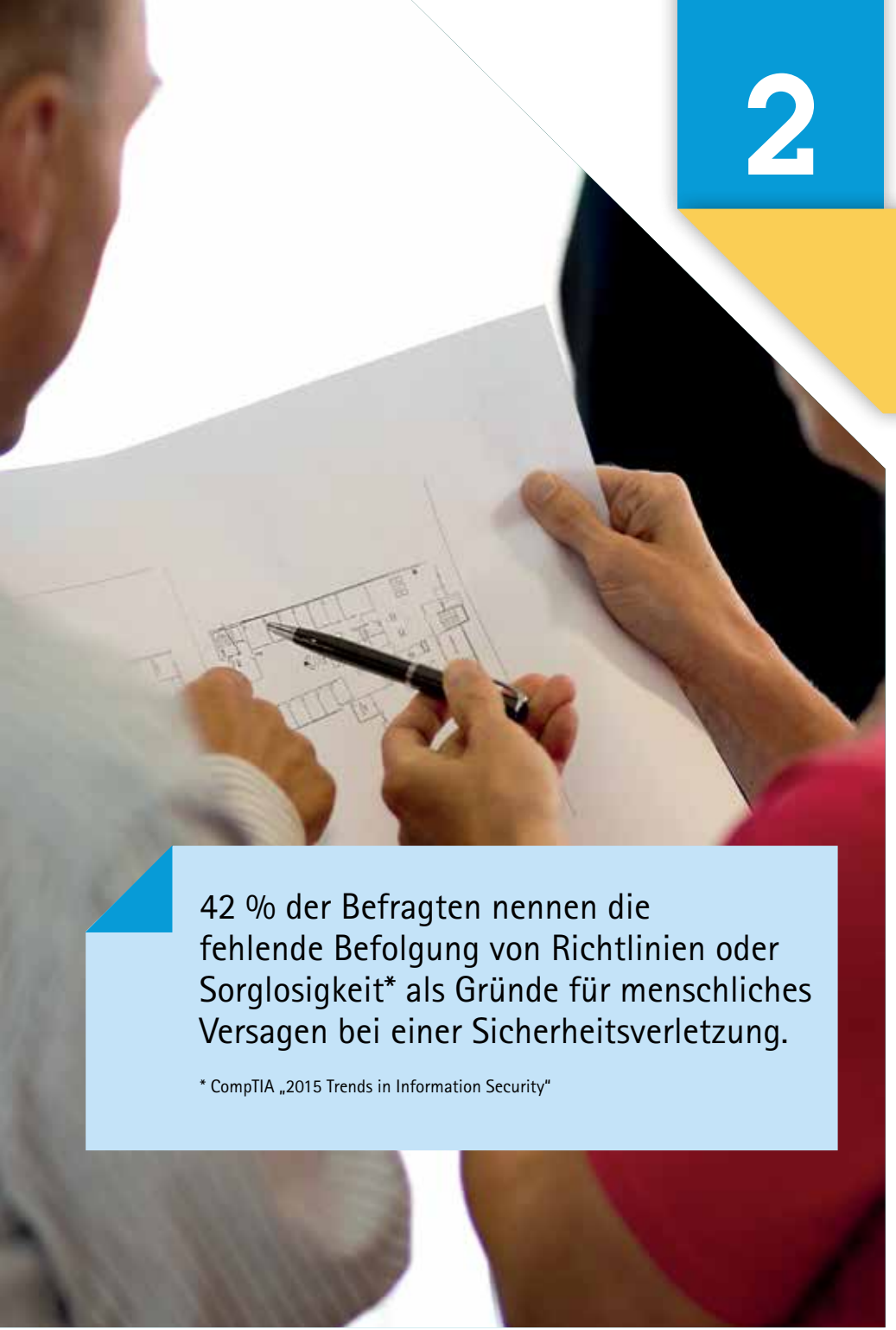
# Ihre IT und Ihr Sicherheitsteam handeln nicht einheitlich

Ihr IT-Team macht sich wahrscheinlich schon seit der Erfindung des Internets durch Al Gore Gedanken über die Cybersicherheit.* IT-Richtlinien gibt es für Ihren Netzwerkbetrieb wahrscheinlich zu Themen wie Kennwortverwaltung und Standard-Netzwerkprotokollen. Doch möglicherweise werden Ihre IT-Richtlinien nicht auf Ihr IP-Überwachungsnetzwerk angewendet.

Häufig sprechen die IT und die Abteilung für Schadensverhütung nicht dieselbe Sprache. Ein einheitliches Handeln ist jedoch wichtig, insbesondere beim Thema Cybersecurity. Klare Hinweise auf mangelnde Einheitlichkeit sind:

> unterschiedliche oder fehlende Richtlinien und Verfahren für heterogene Netzwerke
> eine schlechte oder unklare Kennwortverwaltung
> die fehlende Eigenverantwortung oder Verantwortlichkeit, um Sicherheitsmaßnahmen in allen Systemen zu überprüfen
> für das Versenden von Videostreams über das Netzwerk werden nicht die neuesten und modernsten Verschlüsselungsmethoden angewandt
> Hard- und Sortware Ihres Netzwerks und Ihre IT-Richtlinien sind nicht aufeinander abgestimmt

* Ja, wir wissen, dass er das Internet nicht erfunden hat, aber Sie verstehen, was wir meinen.



42 % der Befragten nennen die fehlende Befolgung von Richtlinien oder Sorglosigkeit* als Gründe für menschliches Versagen bei einer Sicherheitsverletzung.

* CompTIA „2015 Trends in Information Security"

2

# Ihre Netzwerkbenutzer befolgen (oder kennen) die Richtlinien und Verfahren nicht

Verfügen Sie über Richtlinien und Verfahren, um Ihr Netzwerk zu schützen? Sind diese so dokumentiert, dass sie allen Benutzern verständlich sind?

Ein guter Tipp für die IT:
Setzen Sie Ihre IT-Richtlinie durch und sorgen Sie dafür, dass diese auf allen Computern und Servern Ihres Unternehmens befolgt wird.

Fragen, die Sie mit Nein beantwortet haben, sind Symptome für einen schlechten Zustand Ihres Netzwerks, der fatale Folgen für Sie haben könnte. Nachfolgend einige zusätzliche Fragen, die Ihnen helfen, diese Symptome zu diagnostizieren:

> Erhalten Ihre Mitarbeiter regelmäßig Schulungen zu Ihrer IT-Richtlinie?

> Erhalten neue Mitarbeiter ebenfalls eine angemessene Schulung?

> Gibt es spezielle Leitfäden für Mitarbeiter zur Vergabe von Kennwörtern?

3

# Ihre Installations- und Wartungspläne sind nicht klar dokumentiert

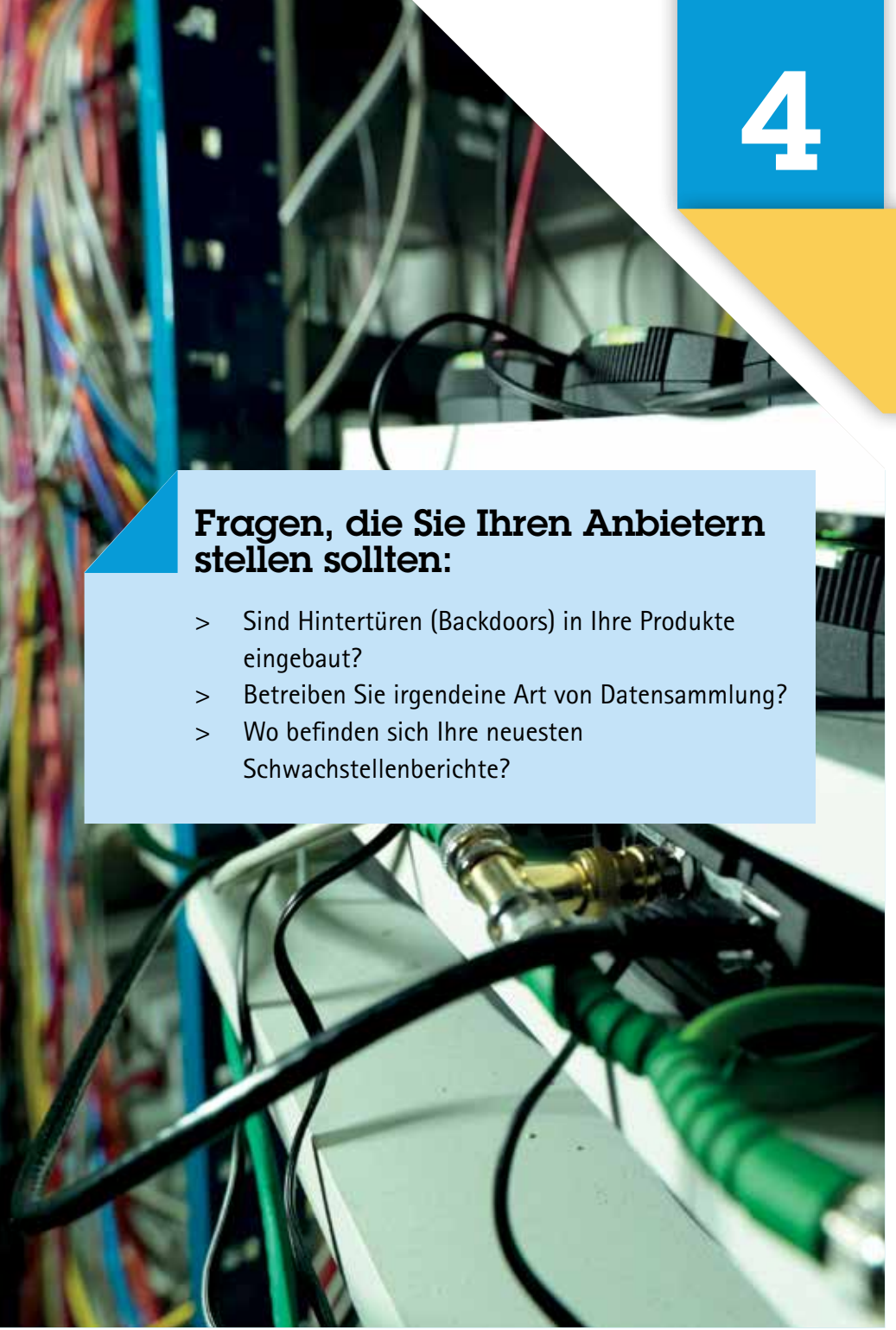
Physische Installation (einer IP-Überwachungskamera oder eines anderen Netzwerkgeräts) und Wartungsprobleme können ebenfalls zu Sicherheitslücken führen. Installateure kennen nicht immer die spezifischen Anforderungen, die sie während der Installation benötigen. Bei einer so großen Anzahl von Anbietern kann es durchaus sein, dass der Installateur eine oder sogar alle bewährten Sicherheitsmethoden außer Acht lässt.

Allzu oft sehen wir leider, dass die Abteilungen für Sicherheit, IT, Gebäude und Wartung keinen einheitlichen Wartungsplan verfolgen. Möglicherweise werden nicht einmal Routinewartungen auf allen Systemen ausgeführt.

Verfügen Sie über einen dokumentierten Plan für die Installation und Wartung aller Ihrer mit dem Netzwerk verbundenen Geräte?

„Das Problem, etwas beim ersten Anlauf richtig zu machen, besteht darin, dass niemand die damit verbundene Komplexität zu schätzen weiß."

- Walter J. Wright



4

# Ihre Technologieanbieter sprechen mit Ihnen nicht über das Thema Cybersicherheit

## Fragen, die Sie Ihren Anbietern stellen sollten:

> Sind Hintertüren (Backdoors) in Ihre Produkte eingebaut?
> Betreiben Sie irgendeine Art von Datensammlung?
> Wo befinden sich Ihre neuesten Schwachstellenberichte?

Erfüllt das von Ihnen ausgewählte Equipment Ihre IT-Richtlinie? Oder versuchen Sie, Ihre Richtlinie an Ihre Anbieter anzupassen? Hier ist Sorgfalt geboten!

In der Zusammenarbeit mit Ihren Technologieanbietern sollten Ihnen die folgenden Punkte zu denken geben:

> Sie sprechen mit Ihnen nicht über das Thema Cybersicherheit
> Sie haben weder Hardening-Guides für Geräte noch Praxisleitfäden
> Sie führen keine Penetrationstests für ihre Produkte durch
> Sie arbeiten nicht mit externen Cybersicherheits-Beratern zusammen, um Produktrisiken zu bewerten

Jede Technologie ist Bestandteil eines größeren Systems. Häufig sind diese Systeme nicht komplett gesichert. Möglicherweise sind nur Teile des Ganzen gesichert, während dies bei anderen nicht möglich ist. Systeme sind nur so stark wie ihre schwächste Verknüpfung. Ist jeder einzelne Teil des Puzzles so sicher wie möglich?

# 10 bewährte Methoden für ein funktionierendes Netzwerk

Wir haben nun herausgefunden, woran ein schlechter Netzwerkzustand zu erkennen ist. Jetzt befassen wir uns mit der Frage, was Sie tun können, um die Cybersicherheit Ihres Netzwerkes zu verbessern. Zusammen mit Ihrer IT, dem Sicherheitsteam und dem Gebäudemanagement können Sie viele der üblichen Risiken minimieren.

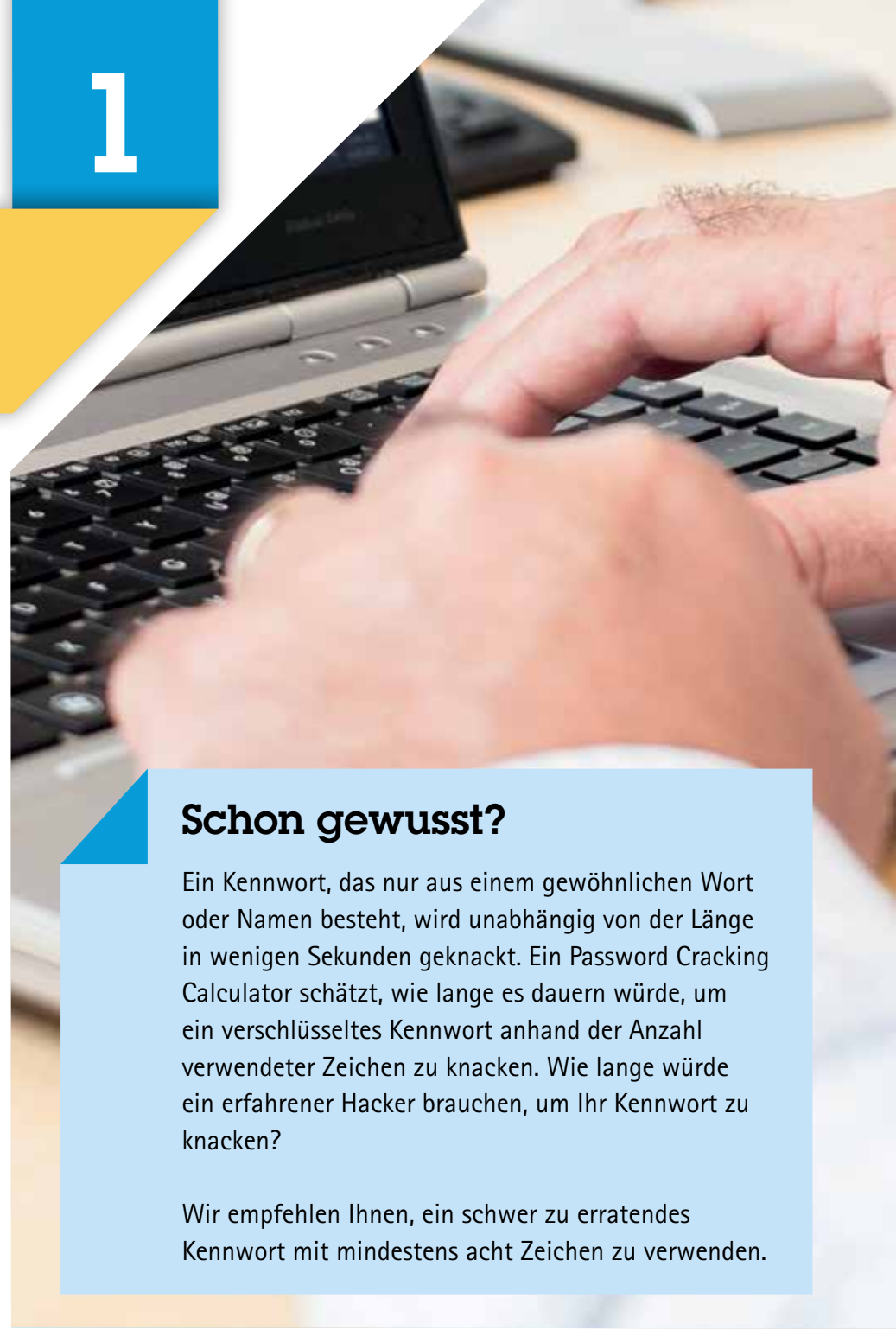
1

# Verwenden Sie sichere, unverwechselbare Kennwörter

Die meisten IT-basierten Geräte werden mit Standardkennwörtern und Standardeinstellungen geliefert. Manchmal lassen sich diese Kennwörter leicht erraten und sind sogar online veröffentlicht. Damit können sich Cyberkriminelle auf einfachem Weg unautorisierten Zugang zu Ihrem System verschaffen.

Achten Sie daher auf die folgenden Punkte:

- richten Sie sichere, unverwechselbare Kennwörter ein
- gewährleisten Sie eine gute Kennwortverwaltung
- verwenden Sie Zertifikate anstelle von Kennwörtern
- ändern Sie Ihre Kennwörter regelmäßig



## Schon gewusst?

Ein Kennwort, das nur aus einem gewöhnlichen Wort oder Namen besteht, wird unabhängig von der Länge in wenigen Sekunden geknackt. Ein Password Cracking Calculator schätzt, wie lange es dauern würde, um ein verschlüsseltes Kennwort anhand der Anzahl verwendeter Zeichen zu knacken. Wie lange würde ein erfahrener Hacker brauchen, um Ihr Kennwort zu knacken?

Wir empfehlen Ihnen, ein schwer zu erratendes Kennwort mit mindestens acht Zeichen zu verwenden.

2

# Installieren Sie Geräte entsprechend den Empfehlungen des Herstellers

Bei der Bereitstellung eines Gerätes aktivierte, aber nicht genutzte Dienste sind eine Schwachstelle für einen Angriff. Beispielsweise könnte ein Cyberkrimineller Schadsoftware und bösartige Scripts über ein File Transfer Protocol (FTP) oder eine Anwendungsplattform von einem nicht vertrauenswürdigen Entwickler installieren. Durch Deaktivieren nicht genutzter Dienste und das ausschließliche Installieren vertrauenswürdiger Anwendungen reduzieren sich die Chancen eines potenziellen Täters, die Schwachstellen eines Systems auszunutzen.

Auch die ordnungsgemäße Installation von Geräten hilft, Sicherheitsprobleme zu vermeiden. Wird beispielsweise eine Kamera in Reichweite einer Person platziert, besteht die Gefahr, dass sie von dieser Person manipuliert oder zerstört wird. Kameras sollten nur dort installiert werden, wo sie den besten Sichtwinkel bieten, um Ihre Szene deutlich zu sehen. Sie sollten sich aber auch außerhalb der Reichweite potenzieller Angreifer befinden.

3

# Definieren Sie klare Zuständigkeiten und Verantwortlichkeiten

In vielen Organisationen kommt es oftmals zu Verletzungen der Netzwerksicherheit, da keine klaren Zuständigkeiten und Prozesse eingerichtet sind, für die Mitarbeiter spezielle Zugriffsrechte haben.

Möglicherweise ist unklar, wer für die Überprüfung von Sicherheitsmaßnahmen von Überwachungssystemen zuständig ist, um so die Einhaltung bewährter Methoden zu gewährleisten. Wir empfehlen Organisationen deshalb, das Least-Privilege-Prinzip anzuwenden. Es besagt, dass Benutzer nur die Rechte erhalten, die zur Erfüllung ihrer jeweiligen Aufgaben erforderlich sind.

Um unautorisierte Zugriffe zu reduzieren, sollten Geräte, die auf Videomaterial zugreifen, nicht die Erlaubnis erhalten, direkt auf Kameras zuzugreifen, außer wenn die Lösung dies erfordert. Kunden sollten nur über ein Video-Management-System (VMS) oder einen Medien-Proxy auf Videomaterial zugreifen können.


4

# Verwenden Sie immer die neueste Firmware

In Betriebssystemen, auf Workstations, Servern, Kameras, Druckern und anderen Netzwerkgeräten gefundene Bugs und Schwachstellen können für Ihr Unternehmen gefährlich werden.

Der bekannte Heartbleed-Bug aus dem Jahr 2014 ist ein gutes Beispiel dafür. Dieser sicherheitsrelevante Programmfehler in OpenSSL ermöglichte es Hackern, den privaten Schlüssel des Serverzertifikats, Benutzernamen und Kennwörter von Servern auszulesen.

Kurz nach dem Bekanntwerden der Schwachstelle wurde ein Patch veröffentlicht. Benutzer, die diesen Patch nicht installierten, waren noch immer gefährdet. Genau aus diesem Grund ist es so wichtig, über einen gut dokumentierten Wartungsplan zu verfügen und die Netzwerkgeräte mit der aktuellen Firmware und allen Sicherheitsupdates immer auf dem neuesten Stand zu halten.

Viele Anbieter publizieren bekannte Schwachstellen und Risikoberichte, die Lösungen oder Workarounds für spezifische Schwachstellen dokumentieren. Verfügen Ihre Geräte über die neueste Firmware?

5

# Führen Sie eine Risikoanalyse durch

Eine Analyse der Cyber-Bedrohungen bestimmt, wie hoch Ihre Gefährdung ist, und wie hoch Ihr Einsatz sein sollte, um sich zu schützen. Erstellen Sie eine Analyse potentieller Bedrohungen inklusive des möglichen Schadens und der Kosten, die Ihnen entstehen, sollte Ihr System angegriffen oder anderweitig kompromittiert werden. Identifizieren Sie Ihre wichtigsten Assets und setzen Sie Prioritäten, um die wertvollsten Assets zu schützen.

Stellen Sie sich folgende Fragen:

- Was muss geschützt werden?
- Wer/Was sind die Bedrohungen und Schwachstellen?
- Welche Folgen hat es, wenn Assets beschädigt werden oder verloren gehen?
- Wie hoch ist der Unternehmenswert

Vergessen Sie keine Schwachstellen in Ihren Assets, die gefährlich für Sie werden könnten. Berücksichtigen Sie bei der Vorbereitung Ihrer Analyse und Festlegung Ihrer Prioritäten sowohl interne als auch externe Bedrohungen.

60 % der Cyberattacken im Jahr 2015 wurden von Insidern durchgeführt. 44,5 % davon wurden als „bösartig" eingestuft.*

* IBM „2016 Cyber Security Intelligence Index"


6

# Informieren Sie sich über Systemschutz und mögliche Bedrohungen

Betrachten Sie nach der Risikoanalyse alle Systeme, die auf Ihrem Netzwerk laufen, genauer. Arbeiten Sie eng mit Ihren Lieferanten zusammen, um über mögliche Bedrohungen Ihres Netzwerk bei der Verwendung Ihrer gewählten Geräte informiert zu sein.

Viele IT-Anbieter bieten mittlerweile dokumentierte bewährte Verfahren oder Leitfäden, um ihre Geräte in Ihrem Netzwerk besser zu schützen (sogenanntes „Hardening"). Wenn die von Ihnen ausgewählten Anbieter Ihnen diese Informationen nicht bereitstellen, sollten Sie dies ansprechen oder andere, nutzergenerierte Dokumentationen eruieren.

Das System sollte als Ganzes betrachtet werden - nicht jedes Gerät für sich. Denn in einem wirklich integrierten System kommunizieren die Geräte miteinander. Idealerweise erfüllen alle Geräte Ihre IT-Richtlinie selbstständig, sobald sie im Netzwerk konfiguriert werden.

7

# Ändern der werksseitigen Standardeinstellungen Ihrer Geräte

Verlassen Sie sich nicht auf die Standardeinstellungen von Geräten. Das gilt insbesondere für das Kennwort. Das Kennwort sollten Sie als erstes ändern. Es ist einer der wichtigsten Schritte, den Sie zum Schutz Ihres Systems unternehmen können.* Denn schließlich sind die Kennwörter das Tor zum gesamten Netzwerk.

Die standardmäßigen IDs und Kennwörter für Adminkonten der meisten Geräte sind über eine einfache Google-Suche leicht zu ermitteln. Der Hacker hat es viel leichter, in Ihr System einzudringen, wenn die werksseitigen Standardeinstellungen beibehalten werden. Aktivieren und konfigurieren Sie unbedingt die Dienste für den Geräteschutz und deaktivieren Sie immer alle Dienste, die Sie nicht nutzen.

Verwenden Sie Standardeinstellungen nur zu Demonstrationszwecken. Selbst das kleinste System ist verwundbar, wenn Standardeinstellungen verwendet werden.

*Ja, das haben wir bereits unter Punkt 1 erwähnt, aber es ist wichtig!

8

# Nutzen Sie verschlüsselte Verbindungen

Die Verbindungen sollten bei allen Netzwerken verschlüsselt sein, auch bei lokalen oder „internen“.

Stellen Sie sicher, dass Ihre Systeme wenigstens eines der üblichen Authentifizierungsprotokolle verwenden: HTTP Digest-Authentifizierung oder HTTPS. Dies gewährleistet, dass alle Informationen vor dem Versenden über das Netzwerk verschlüsselt werden. Diese Protokolle reduzieren effektiv die Wahrscheinlichkeit eines Lauschangriffs, bei dem ein schädlicher Code unverschlüsselte Übertragungen ausspäht. Auch wenn Sie Finanzdaten nicht sichern, sind Ihre Daten doch immer noch wichtig genug, um durch Verschlüsselung gesichert zu werden.

## Mit diesen Informationen beeindrucken Sie Ihr IT-Team!

HTTP Digest-(Access)-Authentifizierung ist ein gängiges Verfahren für Webserver, um Zugangsberechtigungen sowie Benutzeridentität (Benutzernamen oder Kennwort) zu bestätigen.

HTTPS (HyperText Transfer Protocol Secure) ist das gegenwärtig am weitesten verbreitete Protokoll zur Datenverschlüsselung. HTTPS ist identisch mit HTTP, allerdings mit einem wesentlichen Unterschied: Die Daten werden mithilfe von SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) weiter verschlüsselt.

9

# Sichern Sie Ihr Netzwerk

Wird der Netzwerkschutz verletzt, steigt das Risiko, dass sensible Daten ausspioniert werden und Angriffe auf einzelne Server und Netzwerkgeräte erfolgen.

Verstehen Sie die Bedeutung von Firewalls und Filtern. Nehmen Sie sich Zeit, um das Backbone Ihres Netzwerks zu sichern. Dieser Schritt unterstützt Sie bei allen anderen Bemühungen, bewährte Methoden der Cybersecurity zu implementieren.

Arbeiten Sie von der Auswahl eines Systems bis zu seiner Implementierung und Wartung während des gesamten Prozesses mit Ihrem IT-Team zusammen.

10

# Wartung von Systemen und Prozessen

Ein System optimal zu warten ist eine echte Herausforderung - jedoch absolut entscheidend für einen guten Netzwerkzustand.

Überwachen Sie regelmäßig alle Geräte und aktivieren Sie Systembenachrichtigungen, falls vorhanden und unterstützt. Zudem sollten Sie die Zugriffsprotokolle regelmäßig prüfen, um zu erkennen, ob ein unberechtigter Zugriff versucht wurde.

Nach der Umsetzung eines Wartungsplans sollte dieser regelmäßig überprüft und bewertet werden. In einer Welt sich rasch verändernder Technologien werden uns ständig Updates, neue Funktionen oder bewährte Verfahren zur Verfügung gestellt. Dokumentieren Sie Ihre Wartungsverfahren, damit Ihre heutigen und künftigen Kollegen Ihre Prozesse verstehen können.

# Videoüberwachung und Cybersicherheit in der Realität

Haben Sie sich schon einmal gefragt: „Warum interessiert sich Axis Communications für meine Cybersicherheit?“ Ein Überwachungsvideo ist ein wertvoller Datenbestand, und Videos können, wie alle anderen sensiblen Daten, für viele üble Zwecke missbraucht werden. Kriminelle können mithilfe gestohlener Videos hochsensible Asset-Bereiche erkennen, VIP-Mustern folgen oder sogar den Betrieb durch Kamerasabotage stören. Manipulation, Vandalismus und Denial-of-Video-Service-Attacken sind weitere potentielle Bedrohungen.

IP-Überwachungssysteme sind im Local-Area-Network angesiedelt. Sie sind bei jeder IT-Richtlinie zu berücksichtigen. IP-Kameras sind wie alle anderen Geräte, Clients und Server im Netzwerk zu schützen.

Bedrohungen müssen auf einer Systemebene verwaltet werden. Die Cybersicherheit Ihres Unternehmens ist nicht nur Ihre alleinige Angelegenheit. Es ist die Aufgabe der gesamten Lieferantenkette, das Netzwerk sowie dessen Geräte und Dienste zu schützen. Sie sollten sich gemeinsam Gedanken über Personen, Prozesse und Technologien machen.

Die Mehrzahl der Verstöße gegen die Netzwerksicherheit beruhen auf menschlichem Versagen, Vernachlässigung, Fehlkonfiguration und schlechter Wartung. Richtlinien zur IT-Netzwerksicherheit werden nicht immer auch auf Überwachungsnetzwerke angewendet. Es ist jedoch unerlässlich, diese Richtlinien zu berücksichtigen.

Sie haben die Wahl. Entscheiden Sie sich für Hersteller von Videoüberwachungsprodukten, die Sie dabei beraten, wie ein geschütztes Videosystem installiert wird, das Ihren vorhandenen Netzwerkschutz nicht herabsetzt.  Bewältigen Sie gemeinsam mit Ihrem IT-Team und Ihren Lösungsanbietern die Risikoanalyse sowie die Bereitstellung und Wartung des Systems.

# Cybersicherheit als Teil Ihrer Unternehmenskultur

Ein schlechter Netzwerkzustand bereitet Organisationen oft große Probleme. Machen Sie es anders! Berichten zufolge können Sicherheitsrisiken um 30 % zurückgehen, wenn Mitarbeiter hinsichtlich Risiken aus dem Netz gut geschult sind. *

Bilden Sie Allianzen für Cybersicherheit. Je mehr Personen in Ihrer Organisation Ihre IT-Richtlinie kennen, umso besser. Auch Personen außerhalb der Arbeitsgruppe für Cybersicherheit sollten der Richtlinie nicht nur zustimmen und sie befolgen, sondern sie auch vollkommen verstehen.

## BONUS Best Practice!

Ein sicheres Netzwerk aufzubauen und zu warten ist eine Aufgabe, an der viele verschiedene Abteilungen beteiligt sein müssen. Sie können das nicht alleine schaffen. Gibt es erst einmal einen Plan, dann kommunizieren Sie diesen in der ganzen Organisation und sorgen Sie dafür, dass er bei der Auswahl und Installation neuer Geräte im Netzwerk immer beachtet wird.

Wie können Sie Cybersicherheit zu einem festen und gelebten Bestandteil Ihrer Unternehmenskultur machen? Folgende Punkte sind zu berücksichtigen:

- Investitionen in Mitarbeiterschulungen
- Einführung von neuen Mitarbeitern in die vorhandenen Prozesse
- Cybersicherheit zur Chefsache machen
- Wissen über neu entstehende Cyber-Bedrohungen erlangen und bekannte Bedrohungen firmenintern an richtiger Stelle kommunizieren
- Cybersicherheit als entscheidenden Faktor für neue Netzwerkausrüstung etablieren
- Einsetzen einer BYOD-Richtlinie für persönliche Mobilgeräte
- Klare Strategie zur Reaktion auf Verletzungen der Cybersicherheit

Wenn Sie die gesamte Organisation für Ihre Pläne zur Cybersicherheit gewinnen können, befinden Sie sich in einer optimalen Position, um die Sicherheit Ihres Netzwerks und Ihrer Geräte zu gewährleisten.

* 2015 Global Megatrends in Cybersecurity (Rep.). (2015). Ponemon Institute LLC. Durchgeführt von: Ponemon Institute©

# Ganz zum Schluss…

Bedrohungen aus dem Netz nehmen immer stärker zu. Daher wird es auch immer wichtiger, proaktiv für einen guten Zustand Ihres Netzwerks zu sorgen. Mit einem Plan zur Risikominimierung und der Reaktion auf Verstöße ist Ihre Organisation gut darauf vorbereitet, vorhandene Schwachstellen zu schließen und künftige potentielle Hackerangriffe zu vermeiden.

Das Befolgen der Strategien zum Schutz Ihrer Daten und Ihres Netzwerks macht Verletzungen – zeitlich und materiell – schwerer und aufwendiger.

Das sind die wesentlichen Erfolgsfaktoren:

> IT-Richtlinie in allen Netzwerken implementieren, inklusive Überwachungsnetzwerk
> Gesamte Lieferkette einbeziehen
> Benutzerschulungen Priorität einräumen
> Cybersicherheit zu einem Teil Ihrer Unternehmenskultur machen
> Benutzerfreundliche Prozesse definieren
> Das System ordnungsgemäß konfigurieren, aktualisieren und überwachen
> Vorhandene Ressourcen nutzen und Maßnahmen ergreifen

Keine Angst vor Cybersicherheit. Denken Sie daran: Die meisten Angriffe sind nicht erfolgreich. Wir erfahren nur nichts über fehlgeschlagene Angriffe. Solange Sie Maßnahmen zum Schutz Ihrer Daten und Ihres Netzwerks etablieren, arbeiten Sie an der Verbesserung des Netzwerkzustands und vermindern die Gefahr von Verletzungen.

# Wie gut ist der Zustand Ihres Netzwerks und der mit ihm verbunden Geräte?

Hardening Guide

Der Sturm auf die Cybersecurity: eine Infografik

Website Produktsicherheit

SANS-Website

Cybersecurity-Website


AXIS®
COMMUNICATIONS