WALLIX
CYBERSECURITY SIMPLIFIED

IT'S ALL ABOUT ACCESS

IT-SICHERHEIT UND KOSTEN FEST IM GRIFF

ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Full Report

IT'S ALL ABOUT ACCESS
IT-SICHERHEIT UND KOSTEN FEST IM GRIFF

Ruhiger schlafen mit WALLIX: Kontrolle über die Cybersecurity und ihre Kosten zurückerhalten

Vorwort

Mancher kann es schon nicht mehr hören… die zweite Welle der Pandemie, anfangs gerne ironisch als „Pleitewelle" uminterpretiert, ist im Herbst 2020 also da. Ebenso, übrigens, wie das zweite Whitepaper unserer Kampagnen-Reihe rund um das Thema Zugangs- und Zugriffssicherheit.

Man sagt ja, dass eine Krise in vielen Menschen das Beste hervorbringt. In Bezug auf die Controller wird sie das zweifellos – denn angesichts der drohenden oder teilweise schon einsetzenden Rezession ist echte Zahlenzauberei gefragt. War die Pandemie zunächst Prüfstein und Katalysator für digitale Arbeitskonzepte, entwickelt sie sich zusehends zum Härtetest für ökonomische Robustheit.

WALLIX
CYBERSECURITY SIMPLIFIED

IT'S ALL ABOUT ACCESS

„DIE ZEIT DER SCHLAFLOSEN NÄCHTE HAT BEGONNEN – NICHT NUR FÜR DEN CFO, SONDERN AUCH FÜR DEN CISO"

In den vergangenen Monaten zeigte sich ganz deutlich, dass mit der neuen Art des Arbeitens im Remote Business Life auch die Anforderungen an die IT-Sicherheit ganz erheblich gestiegen sind. Im Zuge der digitalen Revolution und der damit einhergehenden Vernetzung immer weiterer Lebensbereiche, mussten die Unternehmen ihre IT-Strukturen für immer neue Interessensgruppen öffnen - Kunden, Partner, Dienstleister – um nur einige zu nennen.

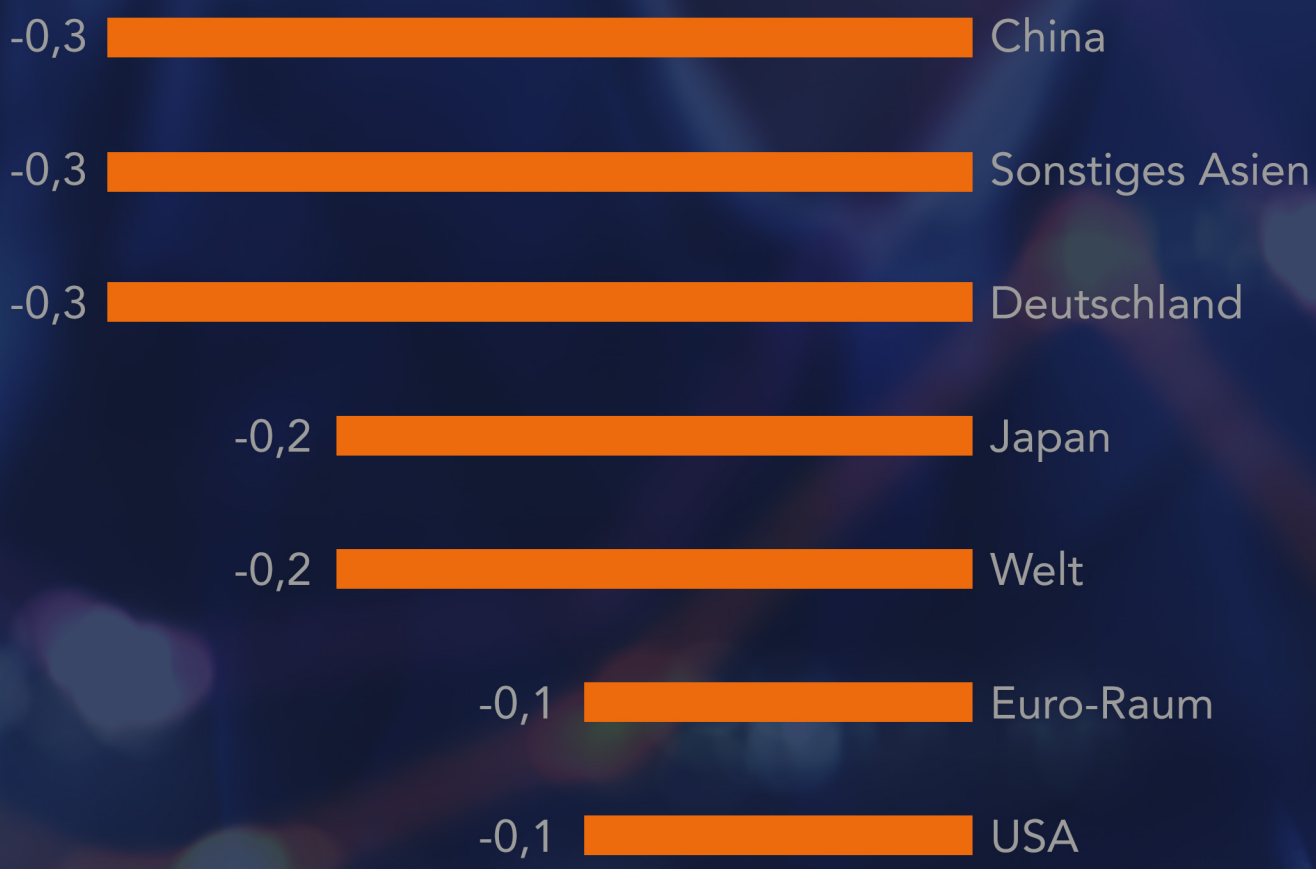
Diese Entwicklung hat nun durch die Pandemie und den nunmehr zweiten Lockdown eine völlig neue Dynamik entwickelt und bereits ein hohes Maß an Investitionskosten verursacht. Für viele Unternehmen rückt das Ende des Fiskaljahres immer näher. Und im gleichen Atemzug entwickelt sich eine wirtschaftliche Gesamtsituation, in der die Zeichen unübersehbar in Richtung Rezession zeigen. Spitze Bleistifte sind nun gefragt und führen auch in den Finanzabteilungen zu einer zweiten Welle: der, der schlaflosen Nächte.

DIE DROHENDE REZESSION - CORONA UND SEINE WIRTSCHAFTLICHEN FOLGEN

Das Wirtschaftsblatt Capital machte die ökonomischen Folgen der Corona-Pandemie bereits im Juni 2020 an fünf Kennzahlen fest: So brach der Export um fast ein Drittel ein, wohingegen bei den Kurzarbeiterzahlen ein Rekordhoch zu verzeichnen war. Auch die Arbeitslosenzahlen stiegen wie auch das Volumen der KfW-Notkredite. Das Bruttoinlandsprodukt wiederum ging um 2,2 Prozent im ersten Quartal im Vergleich zum Vorquartal zurück. Das Statistische Bundesamt bewertete den Abfall als stärksten Rückgang seit der Finanzkrise.

So stark könnte Corona die Wirtschaft schwächen

Prognostizierter Rückgang des BIP 2020 durch Auswirkung des COVID-19-Virus (in Prozenzpunkten)



Quelle: Deutsche Bank via Handelsblatt

WALLIX
CYBERSECURITY SIMPLIFIED

Selbst wenn es sich um eine Bestandsaufnahme aus der Zeit der ersten Corona-Welle handelt: Es steht außer Frage, dass wir am Beginn einer schweren Rezession stehen. Gleichzeitig stehen die Organisationen vor der Herausforderung, ihre IT und die damit aufs Engste verknüpften Sicherheitskonzepte an die neue ituation, die sich aus Entwicklungen wie Remote Work und Digitalisierung ergeben, anzupassen. Gerade beim Thema IT-Security gibt es keine Kompromisse, denn die wirtschaftlichen Folgen von Cyber-Attacken sind eklatant – sowohl in monetärer als auch ideeller Hinsicht.

LEADING FACTORS FOR **CYBERSECURITY SPENDING**	
Driver	Percent Response
Regulatory compliance	69,4
Reducing incidents and breaches	59,1
Keeping up with the evolving threat landscape	56,9
Maintaining our reputation in our industry sector	42,9
Investigating and responding to security events and incidents	40,0
Maintaining adequate security staffing and skills	39,0
Protection of our intellectual property (IP)	33,7
External events impacting other organizations in our industry sector	27,4
Company financial performance or overall economic conditions	26,0
Incidents and breaches that have occurred at our partners	20,8

Abbildung 1: Barbara Filkins, SANS Institut 2020: „IT Security Spending Trends"

DAS IT-SECURITY-DILEMMA: INVESTITIONEN IN SCHUTZVORKEHRUNGEN ERWIRTSCHAFTEN KEINEN GEWINN

Und damit wären wir schon beim ersten Grund, warum die Controller in den Unternehmen nicht mehr gut schlafen.

„Nur eine Minderheit der Unternehmen budgetiert ihre Investitionen in die IT-Sicherheit auf eine eigene, eindeutig identifizierbare Kostenstelle. Das macht die Rechtfertigung dieser Ausgaben schwierig"[1]

Studien belegen, dass zwar zunehmend mehr Geld für IT-Sicherheit ausgegeben wird. Allerdings zeigte sich im Rahmen dieser Umfragen auch, dass nur eine Minderheit der befragten Organisationen die Investitionen in die IT-Sicherheit auf eine eigene, eindeutig identifizierbare Kostenstelle budgetiert. Das macht die Rechtfertigung dieser Ausgaben natürlich schwierig: Das Reporting und Controlling sowie die Steuerung von IT-Sicherheitsinvestitionen werden dadurch fast unmöglich. Somit stehen Unternehmen insbesondere in Zeiten wirtschaftlicher Unsicherheit vor dem Dilemma, einerseits ihre Daten und ihr geistiges Eigentum vor Cyberkriminalität zu schützen und andererseits die dafür notwendigen Investitionen zu begründen, zu planen und zu messen.

[1] *Barbara Filkins, SANS Institut 2020: „IT Security Spending Trends"*
[2] *" z. B. die aktuelle Studie „IT Security Spending Trends" von 2020, von Barbara Filkins, SANS Institut*

Steigende Investitionen

65%
Kollaborations-Tools

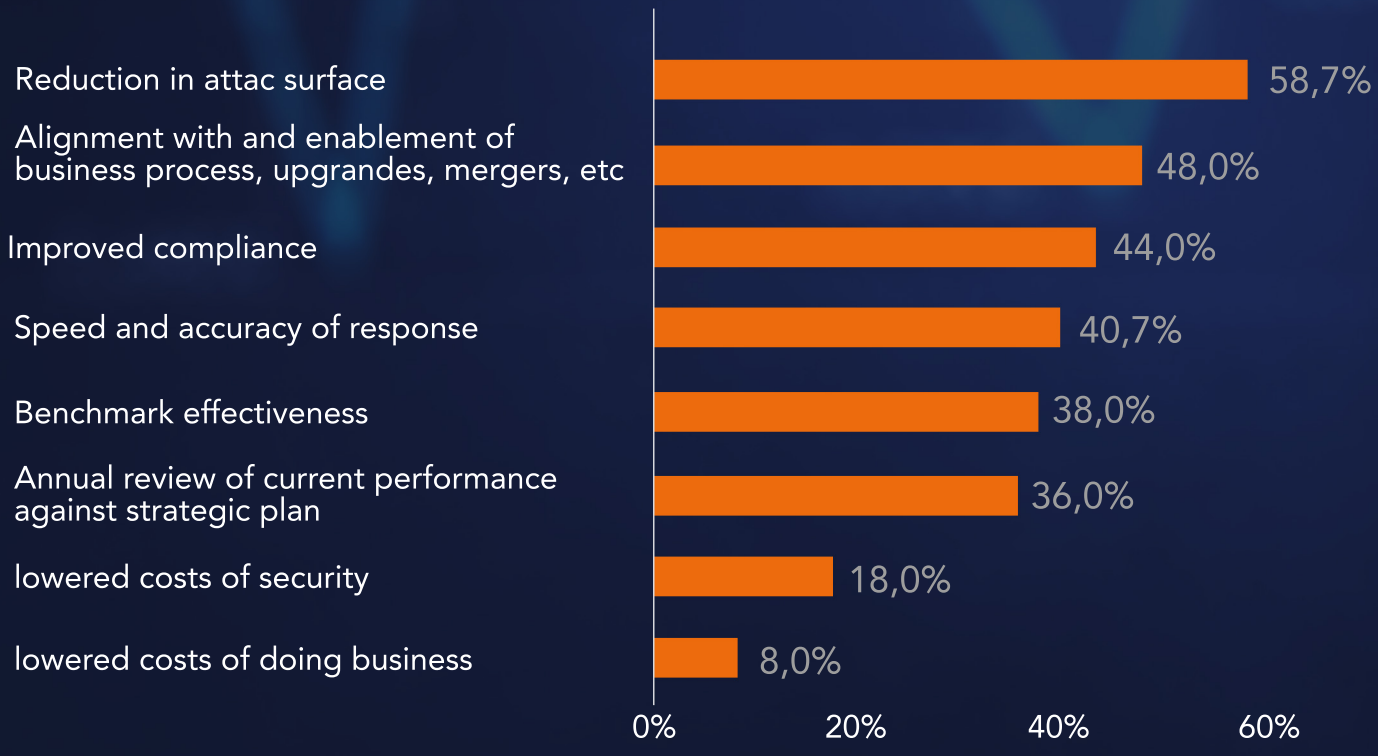
56%
Cyber Security

51%
Cloud

Quelle: TCS COVID-19 Business Impact Survey 2020

How do you evaluate the effevtiveness of your security spending

Select your top three, in no paticular order.



WALLIX
CYBERSECURITY SIMPLIFIED

Drei Wirtschaftlichkeitseffekte von IT-Sicherheit

Dabei steht außer Frage, dass Maßnahmen und Verfahren zur Steigerung der IT-Sicherheit sich auch anderweitig positiv in Unternehmen bemerkbar machen. Praktische Beispiele und belastbares Zahlenmaterial für die Wirtschaftlichkeit von IT-Sicherheitsverfahren fehlen in Deutschland jedoch bislang. Allerdings leuchten die konkreten Mehrwerte von IT-Sicherheitsinvestitionen jedem ein.

Lässt man die negativen Auswirkungen auf die Reputation und das Vertrauen, die dadurch vermieden werden können, einmal beiseite, bleiben drei handfeste, „geldwerte" Vorteile übrig:

- **Die Vermeidung von Schäden und Folgeschäden**
- **Die Steigerung der Effizienz bestehender Verfahren und Bewahrung getätigter Investitionen**
- **IT-Sicherheitsverfahren als Grundlage für neue Anwendungen**

Da ist zunächst einmal wenig überraschend die **Vermeidung von Schäden und Folgeschäden.** Vor allem die Folgen von Cyberattacken lassen sich mitunter kaum überschauen. Strafzahlungen etwa aufgrund von Verstößen gegen gesetzliche Vorschriften zum Datenschutz oder zur Archivierung. Vor allem Betreiber kritischer Infrastrukturen sehen sich hier einer Vielzahl von Regelungen gegenüber, deren Nichteinhaltung teils recht empfindliche Strafen nach sich ziehen. Für alle Organisationen gilt, sind Sicherheitsverletzungen erst einmal passiert und wertvolle Daten – Kundendaten beispielsweise – erst einmal gestohlen, drohen Schadensersatzforderungen.

What is the cost?

$3,9 Mio. is the avergae cost of a data breach.

The average cost per stolen record is $150

88% of companies spent over $1 Mio. on GDPR prep.

WALLIX
CYBERSECURITY SIMPLIFIED

Eine Sicherheitsstrategie, die all das verhindert, beziehungsweise die damit einhergehenden Risiken deutlich minimiert, kann auch in anderer Hinsicht wirtschaftlich sein. Dann nämlich, wenn neue Security-Konzepte **die Effizienz bestehender Verfahren noch einmal deutlich steigern**. Als Beispiel seien hier Autorisierungs- und Authentifizierungs-Lösungen genannt, wie einfach zu bedienende Signaturkarten oder Passwortmanager, die die Effizienz von Arbeitsprozessen optimieren und Produktivität auch in plötzlich dezentralisierten oder neuen Arbeitsprozessen gewährleisten.

Ein weiteres Beispiel für wirtschaftliche Invests ist die sinnvolle Ergänzung des IT-Sicherheitskonzepts: Dreh- und Angelpunkt der Sicherheit ist die Firewall – sie ist die stärkste Verteidigung gegen Cyberangriffe. Die stetig steigende Zahl an Schnittstellen für den Fernzugriff ist dabei ein massives Sicherheitsrisiko. Die Ergänzung der IT-Sicherheit um eine Access Management-Lösung kann diese Sicherheitslücken wieder schließen und durch ein zentrales Zugangsportal ersetzen.

Unnötige Overhead-Lösungen und zusätzliche Folgekosten können durch solche ökonomisch sinnvollen Invests vermieden und die Wirtschaftlichkeit der Neuausgaben optimiert werden.

IT-Sicherheitsverfahren können aber auch – und das liegt nun weniger offensichtlich auf der Hand – **als Grundlage für neue Anwendungen** bis hin zu neuen Geschäftsmodellen dienen. Man nennt das die „enabling"-Rolle von IT-Sicherheit. Dafür sind Public-Key-Infrastrukturen ein Beispiel, ohne die etwa Homebanking oder der elektronische Abschluss von Verträgen gar nicht möglich wäre. Gleichzeitig helfen sie, die Vertraulichkeit und Authentizität der Kommunikation in einem Betrieb und nach draußen effizienter zu gestalten.

„Die Effizienz von Invests in die IT-Sicherheit kann nur gemessen werden, wenn die Zielsetzung zuvor definiert wurde. Dies tun lediglich 35% der Unternehmen. 65% fischen bei ihren Investitionen im Trüben"[3]

IT'S ALL ABOUT ACCESS

WIE KANN WIRTSCHAFTLICHKEIT ERFASST WERDEN?

Schon Archimedes sagte: „Miss alles, was sich messen lässt, und mach alles messbar, was sich nicht messen lässt." Wie aber misst man die wirtschaftlichen Vorteile von Investitionen in die IT-Sicherheit? Indem man Zahlen sprechen lässt – und hier gibt es, wie so oft im Leben, verschiedene Herangehensweisen.

- Da wäre zunächst das Verfahren der **Total Cost of Ownership (TCO)**. Hierbei werden nicht nur die Anschaffungskosten einer Investition berücksichtigt, sondern alle weiteren direkten und indirekten Kosten für Beschaffung, Installation, Wartung, Schulung, kalkulatorische Anteile für Mieten und Energiekosten. Ziel des Verfahrens ist eine möglichst umfassende Sicht auf die Kosten einer Investition. Für eine Wirtschaftlichkeitsbetrachtung ist die Zusammenstellung der Kosten jedoch nur ein Aspekt, zusätzlich ist auch die Ertragsseite zu berücksichtigen.
- Die Rendite von Investitionen berücksichtigt das Konzept des **Return-on-Investment – RoI** genannt. Sie ergibt sich als Quotient aus Gewinn und Kapitaleinsatz. Mit Hilfe dieses Wertes kann die Frage beantwortet werden, wann sich eine Investition amortisiert hat, das heißt, wann die Erträge das eingesetzte Investitionskapital überschreiten.
- Wenn es um die Schätzung der Wirtschaftlichkeit von IT-Sicherheitsinvestitionen geht, wird das Konzept des **Return on Security Investment RoSI** genannt. Es verspricht eine budgetmäßige Kontrolle und eine greifbare Nutzenmessung von IT-Sicherheitsinvestitionen. In die Berechnung des RoSI fließen Kosten für Aufwendungen zur Beseitigung von Schäden durch IT-Sicherheitsvorfälle ein. Der RoSI ist dann positiv, wenn die vermuteten Einsparungen durch das Vermeiden von Schäden größer sind als die Investition in die IT-Sicherheitsmaßnahme.

[3] *Barbara Filkins, SANS Institut 2020: „IT Security Spending Trends"*

DER SPITZE BLEISTIFT UND PRAKTIKABLE ANSÄTZE FÜR DIE JAHRESPLANUNG 2021

Um ein weiteres Zitat zu bemühen: „Lasst schönen Worten Taten folgen." Wo also können Organisationen oder ihre CISOs ansetzen, um die Performance der IT Security-Infrastruktur zu optimieren und gleichzeitig Kosten zu reduzieren?

- **Automatisierung**

Ein Ansatz besteht darin, den Grad der Automatisierung zu erhöhen: Für die Beschleunigung von Prozessen und ein deutliches Plus an Effizienz bietet sich auch für IT-Abteilungen die robotergestützte Prozessautomatisierung (RPA) an. Dadurch werden in vielen Fällen die Mitarbeiter von sich ständig wiederholenden Aufgaben entlastet. Sie können sich in der eingesparten Zeit wertschöpfenderen Aufgaben zuwenden. Die Automatisierung von Teilen des Identitäts- und Zugriffsmanagements (IAM), bei dem in der Regel intensive manuelle Aufgaben anfallen, liefert besonders gute Ergebnisse, ebenso wie die Automatisierung der Reaktionen auf bestimmte Vorfälle.

„Das Risikomanagement ist entscheidender Faktor für die erfolgreiche Kostenreduzierung in der IT-Security. Unternehmen müssen sich auf ihre Hauptrisiken fokussieren und ihre Budgets dafür aufwenden – hier bringt es den größten Nutzen."[4]

- **Optimierung**

Auch das Risikomanagement ist ein entscheidender Faktor für eine erfolgreiche Kostenreduzierung im Bereich IT-Security. Die größten Risiken, denen Unternehmen ausgesetzt sind, werden identifiziert und regelmäßig neu bewertet. Die Investitionen für die IT-Security werden sodann auf die identifizierten Risiken neu ausgerichtet. Das heißt, die Unternehmen müssen sich auf ihre Hauptrisiken fokussieren und ihre Budgets darauf aufwenden, weil es in diesem Bereich den größten Nutzen bringt.

[4] *Barbara Filkins, SANS Institut 2020: „IT Security Spending Trends"*

Die Cyber Kill Chain nach Lockheed Martin beispielsweise ist ein mehrstufiges Modell zur Analyse von Attacken und zum Aufbau der Abwehr entlang der Angriffsschritte. Sie kann beim Risikomanagement wertvolle Dienste leisten.

- **Primäre Verwundbarkeiten**, die bei jedem Cyber-Angriff die elementare Rolle spielen, sind etwa die Schnittstellen für den Fernzugriff – also die Optionen, die es einem Angreifer erlauben, die Perimeter unbemerkt zu passieren und die Möglichkeit, Schadcodes einzuschleusen – also den eigentlichen Angriff durchzuführen.

- Um das zu verhindern, muss zunächst einmal die Basis-Sicherheit wiederhergestellt werden, also die Stärkung der Perimeter zur unüberwindbaren Brandschutzmauer. Dies gelingt, indem zunächst sämtliche Fernzugriffsschnittstellen – jede für sich eine Ausnahme in der Firewall auf Port-Ebene – wieder geschlossen werden. Der Zugang zur internen Infrastruktur kann dann durch einen abgesicherten Zugang über ein sicheres Access Management wie folgt geschützt werden: Sitzungen und auch das aktive Eingreifen bei etwaigen Richtlinienverstößen werden durch das Session Management überwacht.

- Identitätsdiebstähle lassen sich durch ein **sicheres Passwort Management** verhindern. In einem nächsten Schritt gilt es, das **Ausführen von Schadsoftware** zu **blockieren**, also alle **Aktivitäten auf den Zielsystemen nach erfolgtem Zugang abzusichern und zu kontrollieren**. So lässt sich Schadsoftware wirkungsvoll neutralisieren.

Mit all diesen Maßnahmen wird die Angriffskette effektiv und nachhaltig unterbrochen. Weiter verfeinert wird dies mit der Anbindung an ein SIEM. Da ein solches System die Daten und Logfiles, die von den zuvor aufgezählten Security-Lösungen in großen Mengen und teils sehr unterschiedlichen Formaten erzeugt werden, sammeln und auswerten kann. Mit den so gewonnenen Erkenntnissen lassen sich dann weitere Maßnahmen zur Verbesserung der allgemeinen IT-Sicherheitsstrategie festlegen.

„Auch CISOs schlafen mitunter schlecht. Viele klagen über Personalprobleme. Zusätzliches Budget würden sie mehrheitlich für zusätzliches Personal ausgeben."

- **Outsourcing**

Auch CISOs schlafen mitunter schlecht. Viele von ihnen klagen über Personalprobleme, da ihre Teams oft unterbesetzt sind und neue Mitarbeiter schwer zu finden sind. Talente sind zudem oft auch teuer und schwer zu halten. CISOs, die ihr Budget optimieren wollen, sollten ihren Personalbedarf prüfen und feststellen, ob einige Positionen oder Funktionen eventuell ausgelagert werden könnten. Am besten an einen Hersteller, der **Best-of-Breed-Tools** für die verschiedenen Funktionen innerhalb der Sicherheitsumgebung anbietet. Wobei ein **Best-of-Suite-Ansatz**, bei dem nur ein Produkt gleich mehrere Tools umfasst, durchaus die bessere finanzielle Option sein kann. Das heißt, der Best-of-Suite-Ansatz könnte nicht nur die Kosten dämpfen, sondern auch die Zeit für die Schulung der Mitarbeiter verkürzen, da sie dafür nur ein Produkt – und nicht mehrere oder viele – zu erlernen brauchen. Dies hätte die Konsequenz, dass die CISOs gegebenenfalls auch weniger Personal (und damit weniger Kosten) für die Überwachung und Verwaltung eines einzigen Best-of-Suite-Produkts gegenüber mehreren Best-of-Breed-Lösungen beschäftigen müssten.

Nicht immer aber muss das Rad von Grund auf neu erfunden werden. Um bereits getätigte Investitionen zu schützen kann es sinnvoll sein, vorhandene Tools und Systeme, die bereits im Einsatz sind, zu überprüfen. Ausgangspunkt dieser Betrachtungen sollte immer das Zugangsmanagement sein – denn, jedem Sicherheitsvorfall geht immer ein unautorisierter Zugriff voraus. Die Kontrolle und Sichtbarkeit über diese Zugänge zurückzugewinnen sollte deshalb oberste Priorität haben. Denn wer seine Zugriffe kontrolliert, der hat auch seine IT-Sicherheit unter Kontrolle. Eine Tatsache, die gerade jetzt, da sich Unternehmensnetzwerke zunehmend öffnen müssen, an Bedeutung gewinnt. Eine erneute Testung und Bewertung kann zu der Erkenntnis führen, dass es vielleicht Lösungen gibt, welche die gleiche Aufgabe besser oder billiger erfüllen oder aber eine sinnvolle Ergänzung zum Bestand darstellen.

[5] *Barbara Filkins, SANS Institut 2020: „IT Security Spending Trends"*

WALLIX
CYBERSECURITY SIMPLIFIED

„It's all about Access. Denn wer den Access kontrolliert, der kontrolliert die Security. Wer den Access nicht unter Kontrolle hat, wird die Security niemals kontrollieren."

Eine solche Lösungs-Suite bietet beispielsweise WALLIX. WALLIX schützt Identitäten und Zugänge zu IT-Infrastruktur, Anwendungen und Daten gleichermaßen. Die Secure Access Lösungen des europäischen Anbieters WALLIX gewährleisten zudem die Einhaltung der jeweils neuesten IT-Sicherheitsstandards. Sie schützen wirksam vor Cyber-Angriffen, Datendiebstahl und -lecks, die mit gestohlenen Zugangsdaten und erhöhten Privilegien für sensible Unternehmenswerte in Zusammenhang stehen.

Fazit

Schlaflosigkeit und Angstschweiß angesichts anstehender Budgetplanungen können der Vergangenheit angehören. Zumindest im Hinblick auf Investitionen in die IT-Sicherheit, die für jede Form der Digitalisierung unverzichtbar sind. Vor allem vor dem Hintergrund der aktuellen Pandemie-Bekämpfung mit einem erneut steigenden Anteil an Remote Work und Fernzugriffen auf der einen Seite und der drohenden Rezession auf der anderen Seite. „Wer für alles offen ist, kann nicht ganz dicht sein" – Lösungen wie die von WALLIX beweisen, dass es durchaus möglich ist, die IT-Infrastruktur für die zunehmende Vernetzung von allen mit allem offen zu halten und dennoch die Kontrolle über die Zugriffe und Datentransaktionen zu behalten. Und - damit kommen wir zum Anliegen dieses Whitepapers zurück - gleichzeitig auch die Kontrolle über die Kosten nicht zu verlieren.

Wer weiß, dass die Unternehmens-IT mit einem validen, Best-of-Suite-Produkt geschützt ist, das auch noch den Vorzug genießt, von einem europäischen Anbieter zu stammen und US-Amerikanischen Backdoor-Begehrlichkeiten damit einen wirksamen Riegel vorschiebt, und darüber hinaus bestehende Investitionen schützt, kann wahrlich ruhig schlafen.

WALLIX
CYBERSECURITY SIMPLIFIED

Über WALLIX

WALLIX ist ein europäischer sicherheitszertifizierter Hersteller für Cyber-Security Lösungen, um die Zugänge zu IT- und OT-Infrastrukturen zu schützen. WALLIX stellt über das „Zero-Trust"-Modell sicher, dass jeder Benutzer, jede Anwendung und jeder Prozess ausschließlich mit den geringst-notwendigen Berechtigungen auf die Informationen und Ressourcen zugreifen darf, die für seine Zwecke erforderlich sind.
Unsere Technologien basieren auf einer schlanken, einfach zu bedienenden und TCO-optimierten Architektur und lassen sich in jede bestehende Security-Infrastruktur integrieren. Durch Analyse aktueller Angriffsvektoren ermöglicht unser Lösungsansatz die unmittelbare Erhöhung der IT-Sicherheit um 60% -80%, aktives Risiko Management, die Umsetzung einer optimierten Sicherheitsstrategie sowie der Erfüllung sicherheitsrelevanter Compliance-Vorgaben.

ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

www.ipg-group.com

wallix.com/de

WALLIX
CYBERSECURITY SIMPLIFIED