Protective Harmony – wie das Miteinander von IT und Sicherheit die Digital Employee Experience (DEX) stärkt

Konsolidierung und Integration unterschiedlicher Technologien in Cybersecurity-Plattformen sind zentrale Themen, die eine effektive und ganzheitliche Sicherheitsstrategie ermöglichen.

In der heutigen digitalen Ära, in der Unternehmen zunehmend auf technologische Lösungen angewiesen sind, muss die Cybersicherheit im Mittelpunkt jeder strategischen Überlegung stehen. Cyberbedrohungen entwickeln sich ständig weiter und werden immer raffinierter, wodurch herkömmliche Sicherheitsansätze oft unzureichend sind. Um diesen Herausforderungen gerecht zu werden, müssen Unternehmen einen ganzheitlichen Ansatz verfolgen, der sowohl die Konsolidierung als auch die Integration unterschiedlicher Cybersecurity-Technologien umfasst. Dies ermöglicht nicht nur eine stärkere Sicherheitsarchitektur, sondern fördert auch die Effizienz und Effektivität der Abwehrmaßnahmen.

Vorwort

**von Dr. Dennis-Kenji Kipker,, Cyberintelligence Institut*

Ein zentrales Problem der Digitalisierung ist der oftmals fehlende Brückenschlag zwischen der IT-Abteilung und dem Security Department. Traditionell arbeiten diese beiden Abteilungen oft isoliert voneinander, mit unterschiedlichen Prioritäten und Verantwortungsbereichen. Die IT-Abteilung konzentriert sich primär auf die Bereitstellung und Wartung der technischen Infrastruktur, während das Security Department für den Schutz dieser Infrastruktur und der darauf gespeicherten Daten zuständig ist. Diese Trennung führt häufig zu Silos, die die Kommunikation und Zusammenarbeit behindern und somit Schwachstellen in der Sicherheitsstrategie eines Unternehmens schaffen. Dabei ist gerade jetzt ein „Miteinander“ gefordert, denn viele neue Richtlinien und Regularien wie NIS2, DORA oder TISAX fordern mehr Proaktivität – sprich Prävention, wenn es um seine IT-Infrastruktur und dem entsprechenden Sicherheitspaket geht.

Die Konsolidierung und Integration unterschiedlicher Technologien bietet die Möglichkeit, diese Silos zu überwinden und eine kohärente, gut abgestimmte Sicherheitsstrategie zu entwickeln. Durch den Einsatz von integrierten Cybersecurity-Plattformen, die verschiedene Sicherheitslösungen wie Firewalls, Intrusion Detection Systems, Endpoint Protection und mehr miteinander verbinden, können Unternehmen eine zentrale Sicht auf ihre Sicherheitslage gewinnen. Dies erleichtert nicht nur die Überwachung und Verwaltung, sondern ermöglicht auch eine schnellere und effektivere Reaktion auf Bedrohungen.

Ein weiterer Vorteil der Konsolidierung ist die Reduzierung der Komplexität. Viele Unternehmen haben im Laufe der Jahre eine Vielzahl von

Sicherheitslösungen implementiert, die oft nicht nahtlos zusammenarbeiten. Dies führt zu einem erhöhten Verwaltungsaufwand und erschwert die Erkennung und Behebung von Sicherheitsvorfällen. Durch die Konsolidierung dieser Lösungen in einer einheitlichen Plattform können Unternehmen ihre Sicherheitsinfrastruktur rationalisieren und somit die Effizienz steigern.

Darüber hinaus spielt die Integration eine entscheidende Rolle bei der Schaffung eines dynamischen und anpassungsfähigen Sicherheitsnetzwerks. Moderne Cybersecurity-Plattformen sind in der Lage, Daten aus verschiedenen Quellen zu sammeln und zu analysieren, um ein umfassendes Bild der Bedrohungslage zu zeichnen. Dies ermöglicht es den Sicherheitsteams, proaktiv zu handeln und potenzielle Angriffe zu erkennen, bevor sie Schaden anrichten können. Eine enge Zusammenarbeit zwischen IT und Security ist hierbei essenziell, um sicherzustellen, dass die richtigen Daten zur richtigen Zeit verfügbar sind und effektiv genutzt werden können.

Die Transformation hin zu einer konsolidierten und integrierten Cybersecurity-Strategie erfordert jedoch nicht nur technologische Investitionen, sondern auch einen kulturellen Wandel innerhalb des Unternehmens. Es ist wichtig, dass alle Beteiligten, von der Führungsebene bis hin zu den operativen Teams, die Bedeutung der Zusammenarbeit und des Informationsaustauschs erkennen und unterstützen. Schulungen und Sensibilisierungsmaßnahmen können dabei helfen, das Bewusstsein für Cybersecurity zu schärfen und eine Kultur der gemeinsamen Verantwortung zu fördern.

Abschließend lässt sich sagen, dass die Konsolidierung und Integration unterschiedlicher Technologien in Cybersecurity-Plattformen ein wesentlicher Schritt zur Verbesserung der Unternehmenssicherheit ist. Durch den synergetischen Brückenschlag zwischen der IT-Abteilung und dem Security Department können Unternehmen eine robuste, effiziente und anpassungsfähige Sicherheitsstrategie entwickeln, die den Herausforderungen der modernen Cyberbedrohungen gewachsen ist. Eine solche integrierte Herangehensweise stärkt nicht nur die Abwehrkräfte, sondern schafft auch die Grundlage für eine nachhaltige und zukunftssichere IT-Infrastruktur.

Frankfurt am Main, den 12. Juli 2024

IT und Sicherheit – sie lieben und sie hassen sich

IT und Sicherheit sind zwei wesentliche Aspekte eines jeden Unternehmens – sie stehen sich gleichermaßen sowohl in einem Synergieverhältnis als auch einem Spannungsverhältnis gegenüber. Die Sicherheit schützt Informationen, Systeme und Netzwerke vor unbefugtem Zugriff, Nutzung, Änderung oder Zerstörung. IT bezieht sich auf die Verwaltung und Wartung der technologischen Infrastruktur, Hardware, Software und Anwendungen, die das Unternehmen funktionsfähig machen und die Kommunikation ermöglichen. Sowohl Sicherheit als auch IT sind entscheidend für die Leistung, den Ruf und die Einhaltung verschiedener Vorschriften und Standards eines Unternehmens.

Allerdings leben Sicherheit und IT nicht immer in grenzenloser Harmonie. Gelegentlich können sie widersprüchliche Ziele, Prioritäten und Erwartungen haben.

Ein Beispiel aus der Praxis, das jeder kennt und gut nachvollziehen kann: Das Sicherheitsteam ist angehalten, möglicherweise strenge Richtlinien und Kontrollen einzuführen, um potenzielle Bedrohungen oder Sicherheitsverletzungen zu verhindern.
Im Gegensatz dazu möchte das IT-Team den Endbenutzern schnellen und einfachen Zugriff auf technologische Ressourcen und Dienste bieten. Das Sicherheitsteam betrachtet das IT-Team als nachlässig und unverantwortlich. Umgekehrt empfindet das IT-Team das Sicherheitsteam als starr und hinderlich – sozusagen als echten Spielverderber. Real bedeutet das, dass die unterschiedlichen Auffassungen zu Spannungen, Frustration und Misstrauen zwischen den Sicherheits- und IT-Teams führen können, was dann sowohl die allgemeine Sicherheitslage als auch Produktivität des Unternehmens beeinträchtigen kann – also eigentlich doppelt schlimm.

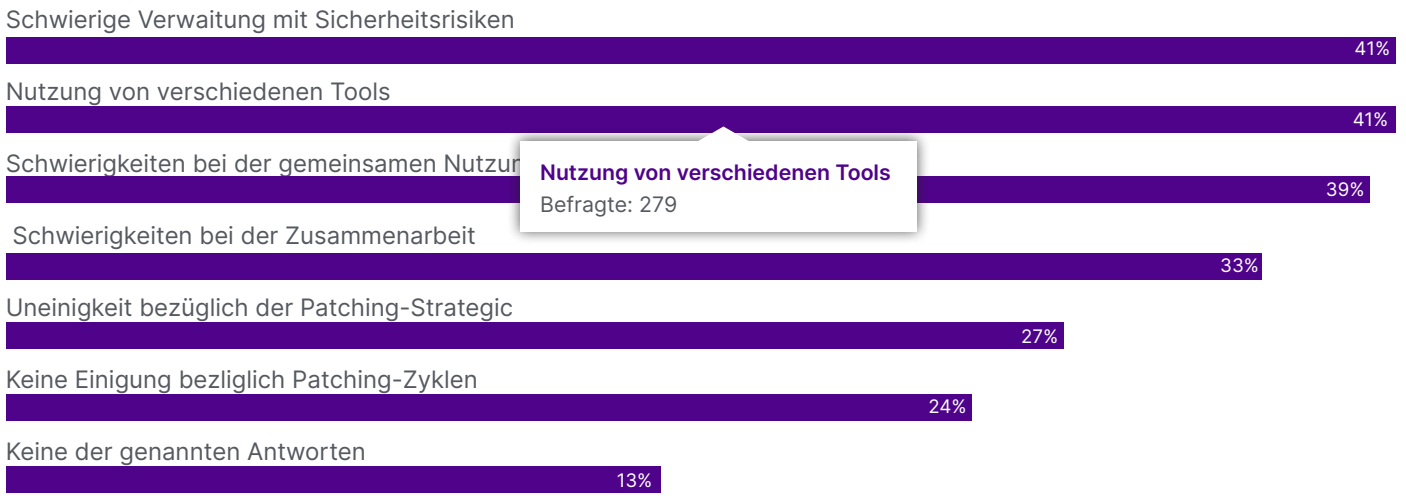
Die Ursachen für das Missverstehen beider Abteilungen

Es gibt viele Gründe, warum Sicherheits- und IT-Teams oft aneinandergeraten:

- **Unterschiedliche Prioritäten:** Sicherheitsteams priorisieren den Schutz von Systemen und Daten. IT-Teams legen jedoch mehr Wert auf Systemleistung, Verfügbarkeit und Benutzererfahrung. Wenn neue Sicherheitskontrollen die Funktionalität oder Benutzerfreundlichkeit beeinträchtigen, entsteht Konfliktpotenzial.
- **Mangel an übergreifendem Wissen:** Sicherheits- und IT-Spezialisten haben oft wenig Einblick in die Bereiche des jeweils anderen. Ohne ein grundlegendes gegenseitiges Verständnis können sich Missverständnisse und Misstrauen entwickeln.
- **Kommunikationsprobleme:** Das schnelle Tempo der technologischen Entwicklung bedeutet oft, dass Probleme unerwartet auftreten und schnelle Reaktionen erfordern. Probleme müssen daher effektiv kommuniziert und voreilige Schlüsse vermieden werden.
- **Unklare Verantwortlichkeiten:** Wenn die Aufgaben zwischen Sicherheit und IT nicht klar definiert sind, herrscht Verwirrung darüber, wer für bestimmte Entscheidungen und Probleme verantwortlich ist. Diese Unklarheit führt dann oft zu Schuldzuweisungen.
- **Ressourcenbeschränkungen:** Begrenzungen in Bezug auf Personal, Budget oder Zugang führen dazu, dass Spannungen über Priorisierungsentscheidungen entstehen.

Auswirkungen der mangelhaften Zusammenarbeit zwischen IT and Sicherheit

F: Welche dieser Herausforderungen sehen Sie in der Beziehung zwischen Sicherheit und IT?



2024 Secure UEM Report | Ivanti
N = 706. Anmerkung: Die Befragten konnten mehrere Optionen auswählen.

Angesichts des Umfangs und der Auswirkungen moderner Cyberbedrohungen müssen wir Wege finden, um sicherzustellen, dass Sicherheits- und IT-Teams nicht gegeneinander arbeiten.

Widersprüchliche Unternehmensanforderungen sind in jeder Organisation normal: Verschiedene Rollen haben unterschiedliche Anforderungen und Prozesse, die sie innerhalb ihrer Abteilungen erreichen. Dennoch werden täglich neue Herausforderungen in der Cybersicherheit entdeckt, die von den Teams bewältigt werden müssen.

Wenn Projekte jedoch voranschreiten und Sicherheitsupdates oder neue Patches veröffentlicht werden, kann dies zu einem zentralen Konflikt zwischen zwei der wichtigsten Faktoren in der IT führen: Verfügbarkeit und Sicherheit.

Der stete Kampf: Verfügbarkeit vs. Sicherheit

IT-Teams haben immer die Verfügbarkeit als oberste Priorität. Ihr Ziel ist es, einen stabilen Betrieb ohne Unterbrechungen zu gewährleisten. Auf der anderen Seite konzentrieren sich Sicherheitsteams ausschließlich darauf, eine sichere Umgebung zu schaffen. Auf lange Sicht kann keines der beiden Teams ohne das andere erfolgreich sein; jedoch verfolgen beide Teams unterschiedliche Ziele.

Zum Beispiel könnte ein Sicherheitsteam die Anforderung stellen, dass Systeme kurzfristig für Patches heruntergefahren werden müssen. Dies gewährleistet eine sichere Umgebung, verringert jedoch die Gesamtverfügbarkeit. Ebenso können Verfügbarkeitsziele wie 99,999 % Betriebszeit zahlreiche Server, Daten und Dienste erfordern, die kontinuierliche Überwachung und Schutz benötigen.

Aufgrund der unterschiedlichen Auffassungen zwischen Verfügbarkeit und Sicherheit gibt es auch Reibungen bei der Wahl der Best Practices, die befolgt werden sollen, wenn Teams zusammengeführt werden. Regelmäßige Systemaktualisierungen und Patches sind sowohl für die Sicherheit als auch für die Leistung des Unternehmens unerlässlich, aber die Art und Weise, wie Patches priorisiert und angewendet werden, kann die Spannungen zwischen IT und Sicherheit verstärken. Wenn die beiden Teams gegeneinander arbeiten – vor allem, wenn die Sicherheitsabteilung der IT-Abteilung eine Anordnung gibt, mit der sie nicht einverstanden ist – entstehen Frustrationen.

Konsolidierung von IT- und Security-Technologien: ein Beitrag zur Harmonisierung

Die Konsolidierung von IT- und Security-Technologien in einer einzigen Plattform bietet eine Vielzahl von Vorteilen. Sie kann die Harmonisierung bei der Abteilung deutlich unterstützen und vorantreiben, was sich dann insbesondere auch auf die Digital Employee Experience (DEX) auswirkt. Wenn IT-Service Management (ITSM), IT-Asset Management (ITAM), Unified Endpoint Management (UEM), Endpoint Security, Network Security und Supply Chain Management integriert werden, entsteht eine umfassende und benutzerfreundliche Lösung, die sowohl die Effizienz als auch die Sicherheit in Unternehmen steigert.

Erhöhte Effizienz und Produktivität

Durch die Integration verschiedener IT- und Sicherheitslösungen in einer einzigen Plattform wird der administrative Aufwand für die Verwaltung und Wartung dieser Systeme erheblich reduziert. Mitarbeiter müssen nicht mehr zwischen verschiedenen Tools und Interfaces wechseln, was Zeit spart und die Produktivität erhöht. Ein einheitliches Dashboard ermöglicht eine zentrale Verwaltung und einen besseren Überblick über alle IT- und Sicherheitsaspekte, was die Effizienz der Arbeitsprozesse verbessert.

Optimiertes Ressourcenmanagement

Mit ITAM und UEM in einer Plattform können Unternehmen ihre Ressourcen besser verwalten und optimieren. Die zentrale Verwaltung von IT-Ressourcen ermöglicht eine genaue Überwachung und Analyse des Ressourcenverbrauchs, was zu einer besseren Planung und Nutzung der vorhandenen Ressourcen führt. Dies hilft, Kosten zu senken und die Effizienz zu steigern.

Verbesserte Benutzererfahrung

Eine konsolidierte Plattform bietet eine einheitliche und intuitive Benutzeroberfläche, die die Bedienbarkeit erleichtert und die Lernkurve für Mitarbeiter verkürzt. Dies führt zu einer besseren Benutzererfahrung, da Mitarbeiter einfacher und schneller auf die benötigten Informationen und Funktionen zugreifen können. Die nahtlose Integration verschiedener Systeme sorgt dafür, dass alle Prozesse reibungslos ablaufen, was die Zufriedenheit der Mitarbeiter erhöht.

Erhöhte Sicherheit

Durch die Konsolidierung von Endpoint Security, Network Security und anderen sicherheitsrelevanten Bereichen in einer einzigen Plattform kann ein ganzheitlicher Sicherheitsansatz verfolgt werden. Sicherheitslücken und Bedrohungen können schneller erkannt und behoben werden, da alle sicherheitsrelevanten Daten zentral erfasst und analysiert werden. Dies führt zu einer höheren Sicherheitslage und reduziert das Risiko von Cyberangriffen und Datenlecks.

Bessere Zusammenarbeit und Kommunikation

Die Integration von ITSM, ITAM und anderen Management-Tools fördert die Zusammenarbeit und Kommunikation zwischen verschiedenen Abteilungen und Teams. Ein einheitliches System erleichtert den Austausch von Informationen und die Koordination von Aufgaben, was zu einer effizienteren Problemlösung und Entscheidungsfindung führt. Mitarbeiter können sich auf eine gemeinsame Plattform verlassen, was die Teamarbeit stärkt und die Gesamtleistung verbessert.

Transparenz und Nachverfolgbarkeit

Eine konsolidierte Plattform bietet eine höhere Transparenz und Nachverfolgbarkeit aller IT- und Sicherheitsprozesse. Alle Aktivitäten und Änderungen werden zentral erfasst und können leicht überwacht und überprüft werden. Dies erleichtert die Einhaltung von Compliance-Vorgaben und gesetzlichen Anforderungen, da alle relevanten Daten und Berichte jederzeit verfügbar sind.

Verbesserte Sicherheit durch strategische Partnerschaften

Auch die Integration von Partnern in das Sicherheits-Ökosystem kann die Sicherheitslage von Unternehmen erheblich verbessern. Indem sie auf das Fachwissen und die fortschrittlichen Ressourcen von Partnern zugreifen und sich damit Zugang zu Spitzentechnologien und branchenspezifischem Wissen verschaffen, das die internen Möglichkeiten möglicherweise übersteigt, können Unternehmen ein breiteres Spektrum von Sicherheitsherausforderungen effektiver angehen. Dieser kooperative Ansatz stärkt nicht nur die Sicherheitsinfrastruktur, sondern fördert auch die Innovation und die Widerstandsfähigkeit gegenüber sich entwickelnden Bedrohungen. Er ist damit eine wichtige Strategie zur Schaffung eines umfassenden und robusten Sicherheitsrahmens.

Unternehmen, die diese Integration umsetzen, können eine robustere, sicherere und benutzerfreundlichere digitale Arbeitsumgebung schaffen, die sowohl den Mitarbeitern als auch der gesamten Organisation zugutekommt.

Die Konsolidierung von IT- und Security-Technologien in eine einzige Lösungsplattform fördert die Harmonisierung zwischen IT und Sicherheit erheblich. Sie ermöglicht eine zentrale Verwaltung und Überwachung, wodurch Kommunikationslücken und Missverständnisse zwischen den Teams reduziert werden. Durch die einheitliche Plattform können Sicherheitsmaßnahmen nahtlos in IT-Prozesse integriert werden, was zu einer höheren Effizienz und schnelleren Problemlösung führt. Mitarbeiter profitieren von einer konsistenten Benutzererfahrung, da sie nicht mehr zwischen verschiedenen Systemen wechseln müssen, was die Produktivität steigert. Insgesamt führt die Konsolidierung zu einer robusteren, sichereren und benutzerfreundlicheren digitalen Arbeitsumgebung.

Eine Harmonisierung führt zu mehr Vertrauen und einer verbesserten Digital Employee Experience (DEX)

Die Harmonisierung von IT und Sicherheit führt zum einen zu mehr Vertrauen in die Digitalisierung und zum anderen auch zu einer besseren gelebten Erfahrung im Umgang mit der IT. Dies wird als Digital Employee Experience (DEX) bezeichnet.

DEX ist die Summe aller digitaler Touchpoints mit denen Mitarbeitende während ihrer Arbeitszeit in Berührung kommen. Es umschreibt wie die Mitarbeitenden die digitalen Möglichkeiten im Unternehmen wahrnehmen. Die DEX bezieht sich auf die Gesamterfahrung, die Mitarbeiter mit den digitalen Tools und Plattformen ihres Unternehmens haben. Ein gut gestalteter DEX kann maßgeblich dazu beitragen, Digital Trust – also das Vertrauen der Mitarbeiter in die digitalen Systeme und deren Sicherheit – aufzubauen.

Eine gut gestaltete Digital Employee Experience spielt also eine entscheidende Rolle beim Aufbau von Digital Trust. Durch Benutzerfreundlichkeit, transparente Kommunikation, Datensicherheit, Zuverlässigkeit, Feedback-Mechanismen und die Integration einer starken Sicherheitskultur können Unternehmen das Vertrauen ihrer Mitarbeiter in die digitalen Systeme stärken. Dies führt nicht nur zu einer höheren Zufriedenheit und Produktivität der Mitarbeiter, sondern auch zu einem insgesamt sichereren und vertrauenswürdigeren digitalen Arbeitsumfeld.

Wie kann man seine DEX verbessern?

Im Grunde genommen geht es bei DEX ja darum, den Mitarbeitenden eine digitale Erfahrung zu bieten, die sowohl Produktivität als auch Arbeitszufriedenheit fördert – und dies kann man aktiv angehen: Der Prozess beginnt mit dem Verständnis Ihrer IT-Umgebung, setzt sich fort mit der Verknüpfung von Patch-Daten, um ein besseres Änderungs- und Sicherheitsmanagement zu ermöglichen, sowie mit der Automatisierung der IT-Workflows , und führt schließlich zur kontinuierlichen Verbesserung, die es ermöglicht, die strategische Entscheidungsfindung im gesamten Unternehmen stetig zu optimieren.

Mit einem guten Einblick in die digitale Mitarbeitererfahrung muss man nicht mehr über die Ursachen von Problemen rätseln, die Ihre den betreffen. Ein effizientes Patch-Management wird ein großes, immer wiederkehrendes Problem für User und IT gleichermaßen lösen und gleichzeitig die Sicherheit erhöhen. Wenn die DEX-Verbesserungen schrittweise umgesetzt werden, summieren sich die Vorteile allmählich. Die Automatisierung von IT-Workflows ermöglicht, Probleme zu lösen, bevor die User sie überhaupt bemerken, und gibt First- Level-Analysten den Kontext, den sie benötigen, um die eingehenden Tickets schnell zu bearbeiten, ohne sie eskalieren zu müssen. Auf diese Weise verbessern sich die KPIs, die IT-Abteilung gewinnt das Vertrauen ihrer Kollegen im gesamten Unternehmen und Ihre IT-Führung hat mehr Flexibilität, um übergeordnete strategische Prioritäten zu verfolgen.

In einem breiteren Verständnis bedeutet DEX-Management:

- Einsatz von Technologien zur Gestaltung zufriedenstellender, komfortablere und effektiver digitaler Erlebnisse für Mitarbeitende, unabhängig von ihrem Alter, ihren technischen Kenntnissen oder ihrem Arbeitsplatz.
- Bereitstellung von Erlebnissen, die sich positiv auf die Sicherheislage eines Unternehmens auswikern.
- DEX wird von einer technischen Anschaffung zu einer umfassenden Philosophie zur Unterstützun der Mitarbeitende und zur Verbesserung der Sicherheit am Arbeitsplatz.

Harmonie erhöht die DEX und kreiert Vorteile

Die Harmonisierung zwischen IT und Sicherheit hat erhebliche Vorteile für die Digital Employee Experience (DEX). Sie führt zu einer stabileren und sichereren Arbeitsumgebung, verbessert die Benutzerfreundlichkeit und erhöht das Vertrauen der Mitarbeiter in die digitalen Systeme. Durch klare Kommunikation, definierte Verantwortlichkeiten und eine Sicherheitskultur, die Zusammenarbeit und gemeinsame Ziele betont, können Unternehmen eine positive und produktive digitale Arbeitsumgebung schaffen.

Die Vorteile im Überblick:

1. Verbesserte Systemverfügbarkeit und Zuverlässigkeit

- ***Reduzierte Ausfallzeiten:*** Durch eine enge Zusammenarbeit zwischen IT- und Sicherheitsteams können Wartungsarbeiten und Sicherheitsupdates besser koordiniert werden, was zu weniger ungeplanten Ausfallzeiten führt.
- ***Stabile Arbeitsumgebung:*** Ein harmonisiertes Team stellt sicher, dass Sicherheitsmaßnahmen ohne Beeinträchtigung der Systemleistung implementiert werden, wodurch die Zuverlässigkeit der digitalen Tools erhöht wird.

2. Erhöhte Sicherheit ohne Produktivitätsverlust

- ***Security by Design:*** Wenn Sicherheit von Anfang an in den Entwicklungs- und Implementierungsprozess einbezogen wird, können Sicherheitsmaßnahmen nahtlos integriert werden, ohne die Benutzerfreundlichkeit zu beeinträchtigen.
- ***Minimierte Störungen:*** Durch die gemeinsame Planung von Sicherheitsupdates und -patches können diese zu Zeiten durchgeführt werden, die die Produktivität der Mitarbeiter nicht stören.

3. Bessere Benutzerfreundlichkeit

- ***Gleichgewicht zwischen Sicherheit und Benutzererfahrung:*** Eine enge Zusammenarbeit ermöglicht es, Sicherheitsmaßnahmen zu entwickeln, die die Benutzererfahrung nicht beeinträchtigen. Zum Beispiel können Multifaktor-Authentifizierungsprozesse so gestaltet werden, dass sie sicher und gleichzeitig benutzerfreundlich sind.
- ***Kontinuierliche Verbesserung:*** Durch regelmäßiges Feedback von beiden Teams können Systeme und Sicherheitsmaßnahmen kontinuierlich verbessert und an die Bedürfnisse der Benutzer angepasst werden.

4. Klarere Kommunikation und Verantwortlichkeiten

- ***Transparenz:*** Durch regelmäßige Meetings und klare Kommunikationskanäle zwischen IT und Sicherheit werden die Mitarbeiter besser über geplante Änderungen und deren Auswirkungen informiert.
- ***Verantwortlichkeiten:*** Klare Rollen und Zuständigkeiten verhindern Missverständnisse und fördern eine reibungslose Zusammenarbeit, was zu einer effizienteren Problemlösung führt.

5. Erhöhtes Vertrauen der Mitarbeiter in die digitalen Systeme

- ***Vertrauenswürdige Systeme:*** Wenn Mitarbeiter sehen, dass Sicherheits- und IT-Teams gut zusammenarbeiten, fühlen sie sich sicherer und vertrauen den digitalen Systemen mehr.
- ***Positive Sicherheitskultur:*** Eine harmonisierte Beziehung zwischen IT und Sicherheit fördert eine Kultur, in der Sicherheit als gemeinsames Ziel angesehen wird, was das Vertrauen der Mitarbeiter in die Sicherheitsmaßnahmen stärkt.

6. Effizientere Problemlösungen

- ***Schnellere Reaktionszeiten:*** Bei sicherheitsrelevanten Vorfällen oder technischen Problemen können gut koordinierte Teams schneller reagieren und Lösungen implementieren.
- ***Proaktive Maßnahmen:*** Durch gemeinsame Analysen und Überwachungen können potenzielle Sicherheitsbedrohungen frühzeitig erkannt und behoben werden, bevor sie die Benutzererfahrung beeinträchtigen.

Fazit

Die Harmonisierung zwischen IT und Sicherheit ist entscheidend für die Optimierung der Digital Employee Experience. Durch die enge Zusammenarbeit beider Abteilungen können Unternehmen eine sicherere, stabilere und benutzerfreundlichere digitale Arbeitsumgebung schaffen, was zu weniger Ausfallzeiten und höherer Produktivität führt. Integrierte Sicherheitsmaßnahmen und Lösungsplattformen minimieren Störungen, während regelmäßige Meetings und klar definierte Zuständigkeiten eine effiziente Problemlösung fördern. Das Vertrauen der Mitarbeiter in die digitalen Systeme steigt, wenn Sicherheits- und IT-Teams harmonisch zusammenarbeiten, was die allgemeine Zufriedenheit und das Sicherheitsbewusstsein stärkt. Auch die Konsolidierung auf Produktseite spielt eine große Rolle. Mit einer integrierten Lösungsplattform können Sicherheitsmaßnahmen nahtlos in IT-Prozesse integriert werden, was zu einer höheren Effizienz und schnelleren Problemlösung führt.

Über Ivanti

Ivanti macht den Everywhere Workplace möglich. Im Everywhere Workplace nutzen Mitarbeiter unzählige Geräte, um über verschiedene Netzwerke auf ITNetzwerke, Anwendungen und Daten zuzugreifen und so von überall aus produktiv arbeiten zu können. Die Ivanti- Automatisierungsplattform verbindet die branchenführenden Unified-Endpoint- Management-, Zero-Trust-Sicherheits- und Enterprise-ServiceManagement-Lösungen des Unternehmens und bietet Unternehmen eine zentrale Plattform für die Selbstheilung und Selbstsicherung von Geräten sowie für den Self-Service von Endanwendern. Mehr als 40.000 Kunden, darunter 96 der Fortune 100, haben sich für Ivanti entschieden, um ihre IT-Assets von der Cloud bis zum Edge zu erkennen, zu verwalten, zu sichern und zu warten und ihren Mitarbeitern ein hervorragendes Endbenutzererlebnis zu bieten, egal wo und wie sie arbeiten. Weitere Informationen finden Sie unter ivanti.de

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.