ivanti

Von Gegenspielern zu Partnern

5 Möglichkeiten, Ihr Sicherheitsteam mit dem IT-Team zusammenzubringen

Gemeinsame Aufträge - aber unterschiedliche Ansätze

Obwohl sowohl die Sicherheits- als auch die IT-Teams das Ziel haben, den reibungslosen Betrieb ihres Unternehmens aufrechtzuerhalten, nähern sich beide Teams dieser Aufgabe aus unterschiedlichen Richtungen: das Sicherheitsteam möchte negative Auswirkungen vermeiden, und das IT-Team möchte die Gesamtleistung verbessern

Aufgaben im Unternehmen: Sicherheit versus IT

Sicherheit verhindert Betriebsunterbrechungen

Das bedeutet, dass Sicherheitsfachleute das Risiko unerwarteter Unterbrechungen aufgrund von Cyberangriffen durch interne oder externe Bedrohungen durch eine Vielzahl kontinuierlicher taktischer Implementierungen und strategischer, proaktiver Bedrohungsanalysen und -beseitigung kontinuierlich minimieren.

IT fördert den operativen Output

Das heißt, IT-Fachleute steigern die Produktivität der User durch nahtlose Technologieimplementierungen und -wartung im Hintergrund, indem sie Hardware- und Softwareprobleme beheben, die den Output und die Ergebnisse anderer Fachleute gefährden.

Wenn die beiden Abteilungen jedoch zusammenarbeiten, können beide ihre Ziele effektiver erreichen.

Die Prozesse funktionieren gut, wenn die IT-Abteilung die Sicherheitsteams unterstützt und proaktive Strategien und Prozesse vorhanden sind, bevor die Sicherheitsabteilung eine Anfrage an ihre IT-Partner stellt.

Aber wie können Sie die Ziele Ihres Sicherheitsteams und die vorgeschlagenen Projekte so präsentieren, dass Sie aktive Unterstützer in der IT gewinnen, die die Sicherheitsrichtlinien erfolgreich umsetzen wollen - und sich nicht versehentlich passive Gegner schaffen, die bereit sind, ihre Sicherheitsziele für ihre eigenen internen Prioritäten zu opfern?

ivanti

Die drei wichtigsten Vorteile einer Allianz aus Sicherheits- und IT-Abteilung

Schnellere, bessere Ergebnisse

Das IT-Team wird Aktualisierungen und Patches, die Zeit und Ressourcen erfordern, eher einführen, wenn es dem Sicherheitsteam, das diese Patches fordert, vertraut.

Gemeinsame Ressourcen, die die Gesamtausgaben für Technik senken

Wenn Teams einander vertrauen, können sie dieselben Tools nutzen, um unterschiedliche Ziele zu erreichen. Durch die gemeinsame Nutzung von Ressourcen werden die Kostenstellengemeinkosten eines Unternehmens reduziert.

Realistische und nachhaltige Sicherheitspraktiken

Die Sicherheitsabteilung hängt von der IT-Abteilung ab, wenn es um die Implementierung von Sicherheitsprotokollen geht. Wenn die Anforderungen zu schwer zu erfüllen sind oder die IT-Abteilung zu viel Zeit kosten, kann die IT-Abteilung diese Vorschriften und Protokolle möglicherweise nicht einhalten.

In diesem eBook zeigen wir Ihnen, wie es geht:

01 **Erläuterung der Gründe für Sicherheitspläne, -änderungen und -anforderungen** vor der Implementierung - sowohl für IT-Administratoren als auch für User.

02 **Die Reduzierung der Sicherheitsrichtlinien hat Auswirkungen** auf die Budgets, Zeitpläne und Ressourcenzuweisungen der IT-Abteilung.

03 **Kompromisse eingehen,** wo immer sich die Sicherheit Flexibilität leisten kann. (Lassen Sie nicht zu, dass das Sicherheitsteam die Abteilung für Nein ist!)

04 **Entwicklung und Durchsetzung gemeinsamer Ziele** mit einer gemeinsamen Sprache, gemeinsamen Dashboards und Metriken, wo immer möglich.

05 **Proaktives Anbieten von Hilfe** – sei es in Form von Verwaltungsaufgaben, technischem Fachwissen, gemeinsamen Ressourcen oder anderem.

Schließlich sitzen alle im gleichen Boot, und sowohl Ihr Sicherheitsteam als auch die IT-Abteilung haben das gleiche Ziel: einen produktiven, sicheren Arbeitsplatz.

ivanti

01

Die Gründe nennen:

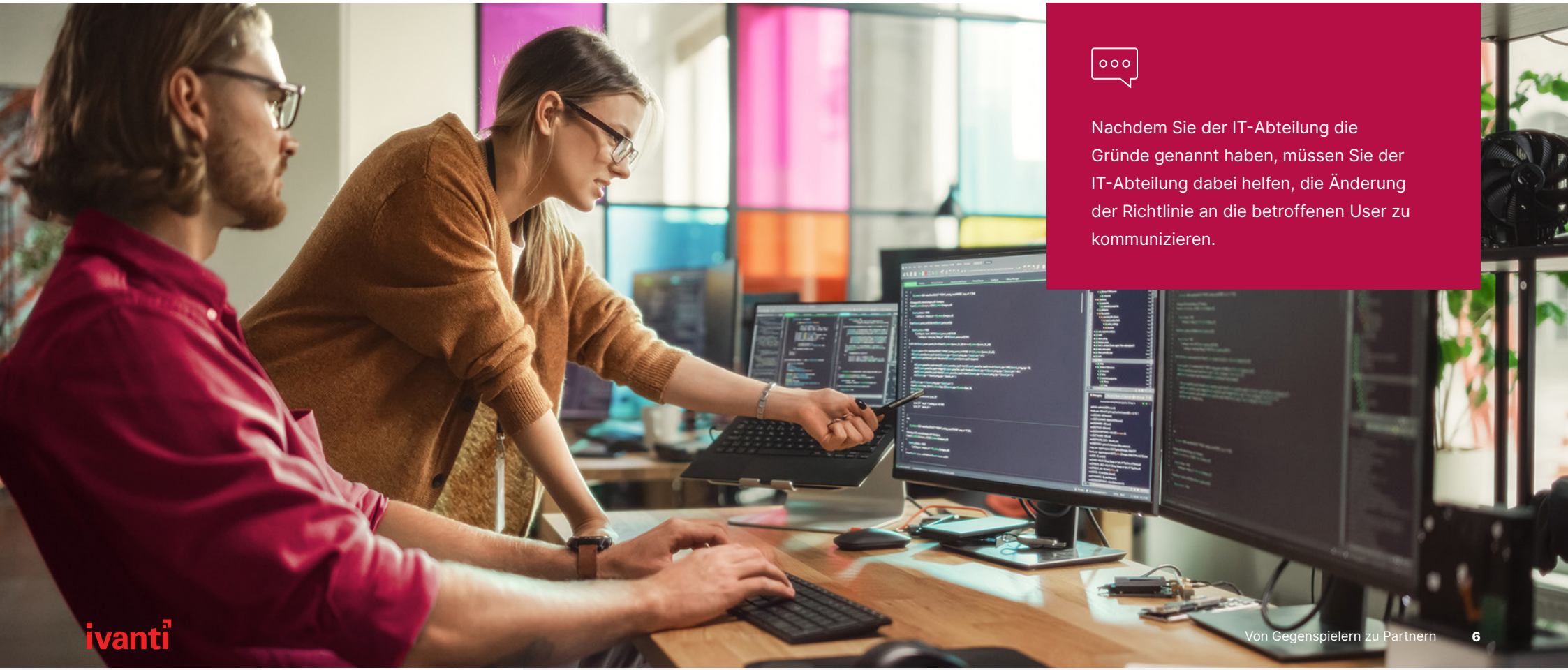
Vermeiden Sie es, Vorgehensweisen einfach zur anzuordnen und bieten Sie Erklärungen für Sicherheitspläne, -änderungen und -anfragen.

ivanti

Erläutern Sie immer die Gründe

Nicht erläuterte Anordnungen der Sicherheitsabteilung bringen IT-Abteilungen schnell in Bedrängnis. Aus Zeit- und Bandbreitenzwängen heraus werden Sicherheitsanfragen gestellt, ohne zu erklären, warum die Änderung beantragt wird, oder ohne zu überlegen, wie die IT-Partner sie umsetzen können.

Wenn Ihr Sicherheitsteam beispielsweise beschließt, Wechselspeichergeräte zu deaktivieren, muss die Umsetzung der Richtlinie wahrscheinlich mit einer Mitteilung an die IT-Abteilung beginnen, um die Gründe dafür zu erläutern. Sie könnten dem IT-Team sagen, dass Ihr Unternehmen durch die Deaktivierung bestimmter Gerätetypen weniger für die Cyberversicherung zahlen muss, Datenverluste durch interne und externe Bedrohungen verhindern und das Risiko für das Unternehmen verringern wird.



Nachdem Sie der IT-Abteilung die Gründe genannt haben, müssen Sie der IT-Abteilung dabei helfen, die Änderung der Richtlinie an die betroffenen User zu kommunizieren.

Ihre gemeinsame Mitteilung sollte Folgendes enthalten:

Eine klare Erklärung der Auswirkungen ohne Verwendung von Fachjargon. So sind in der internen Formulierung einer Richtlinie zum Verbot von Geräten beispielsweise Begriffe wie „Sprunglaufwerke“, „USB-Laufwerke“ oder „alles, was Dateien enthalten kann und mit einem Kabel an den Computer angeschlossen wird“ anstelle von „Wechselspeichergeräten“ empfehlenswert

- Die Richtlinie sollte auch klarstellen, was nicht betroffen ist - in diesem Fall kabelgebundene Computermäuse, Tastaturen, Lautsprecher und andere Peripheriegeräte.

Bieten Sie einen klaren Zeitplan mit einer Vorankündigung von mehr als ein oder zwei Tagen an, damit die User Zeit haben, alternative Vorkehrungen zu treffen und nicht versehentlich USB-Laufwerke von Laptops vor einer wichtigen Verkaufspräsentation zu sperren.

Definieren Sie Ausnahmen von der Aufgabe – und ein hoffentlich problemloses Verfahren für die Beantragung dieser Ausnahmen -, um die User davon abzuhalten, für ihre „einzigartige Situation“ Umgehungslösungen zu finden

Bestimmen Sie wichtige Stakeholder oder Standorte , die die zu erwartenden häufig gestellten Fragen beantworten, häufig auftretende Probleme beheben und unerwartete Sonderfälle behandeln können.

Ohne diese Kommunikation würde das IT-Team bei der Einführung des Sicherheitsprotokolls mit Beschwerden und Tickets überflutet werden - und diese Frustration und dieser Ärger könnte sich dann am Sicherheitsteam entladen.

02

Auswirkungen minimieren:

Die Reduzierung der Sicherheitsrichtlinien hat Auswirkungen auf die Budgets, Zeitpläne und Ressourcenzuweisungen der IT-Abteilung.

ivanti

Auswirkungen auf die IT voraussehen und minimieren

Seien Sie sich bewusst, welche anderen Anforderungen an das IT-Team gestellt werden. Es kann sein, dass sie zum Zeitpunkt Ihrer Anfrage mit einem größeren Projekt beschäftigt sind oder dass sie nicht die nötigen Mitarbeitenden haben, um die Aufgabe zu erledigen.

Suchen Sie stattdessen nach Tools und Systemen, die Ihren IT-Mitarbeitenden die Umsetzung von Sicherheitsrichtlinien, -anforderungen und -korrekturen erleichtern - und gehen Sie nicht so vor, wie sich das Sicherheitsteam üblicher gegenüber der IT-Abteilung verhält.

Auswirkungen auf die reale Welt

Die Sicherheitsabteilung einer Universität zwang die IT-Abteilung, Studierenden temporäre 24-Stunden-Passwörter zuzuweisen

Das Sicherheitsteam einer Universität beschloss, eine gerätegebundene zweistufige Verifizierung für alle User auf dem Campus einzuführen - einschließlich aller Studierenden, die ihre Geräte häufig verlegen oder verlieren würden.

Wenn ein Studierender oder eine Studierende ein vorübergehendes neues Passwort für den Zugang zum Universitätsnetz und zu den Ressourcen beantragen musste, war das Sicherheitsteam gefordert:

1. Eine persönliche Überprüfung der Identität des Antragsstellenden - entweder persönlich oder per Zoom-Telekonferenz.
2. In der Sitzung wies sich der Antragsstellende offiziell aus und beantwortete mehrere Sicherheitsfragen.
3. Dann konnte das Team vorläufige Ausweise ausstellen, die nur 24 Stunden gültig waren.
4. Wenn ein Schüler bzw. eine Schülerin in dieser Zeit sein bzw. ihr altes Gerät nicht wiederfindet - oder einfach ein neues bekommt -, muss er bzw. sie den gesamten Prozess noch einmal durchlaufen!

Hätte sich das Sicherheitsteam die Mühe gemacht, die IT-Abteilung zu konsultieren, bevor es die lästige Richtlinie einführte, hätte es erkannt, dass die elegantere Lösung gewesen wäre, das Netzwerk aufzuteilen,

- indem man ein begrenzteres Studentennetz mit einfacheren Authentifizierungen eingerichtet hätte;
- indem man den vollständigen Interview- und Wiederherstellungsprozess für ein sensibleres Mitarbeiternetzwerk beibehalten hätte.

Schließlich haben erfahrene Mitarbeitende in der Regel einen größeren Anreiz und mehr Möglichkeiten, den Überblick über ihre Geräte zu behalten, als jüngere Studierende an Universitäten.

Ein solches geteiltes Netzwerksystem hätte den Bedürfnissen der IT-Abteilung Rechnung getragen und gleichzeitig die persönlichen Geräte der Studierenden trotz der häufigen Verluste , z. B. auf Uni-Partys. gesichert.

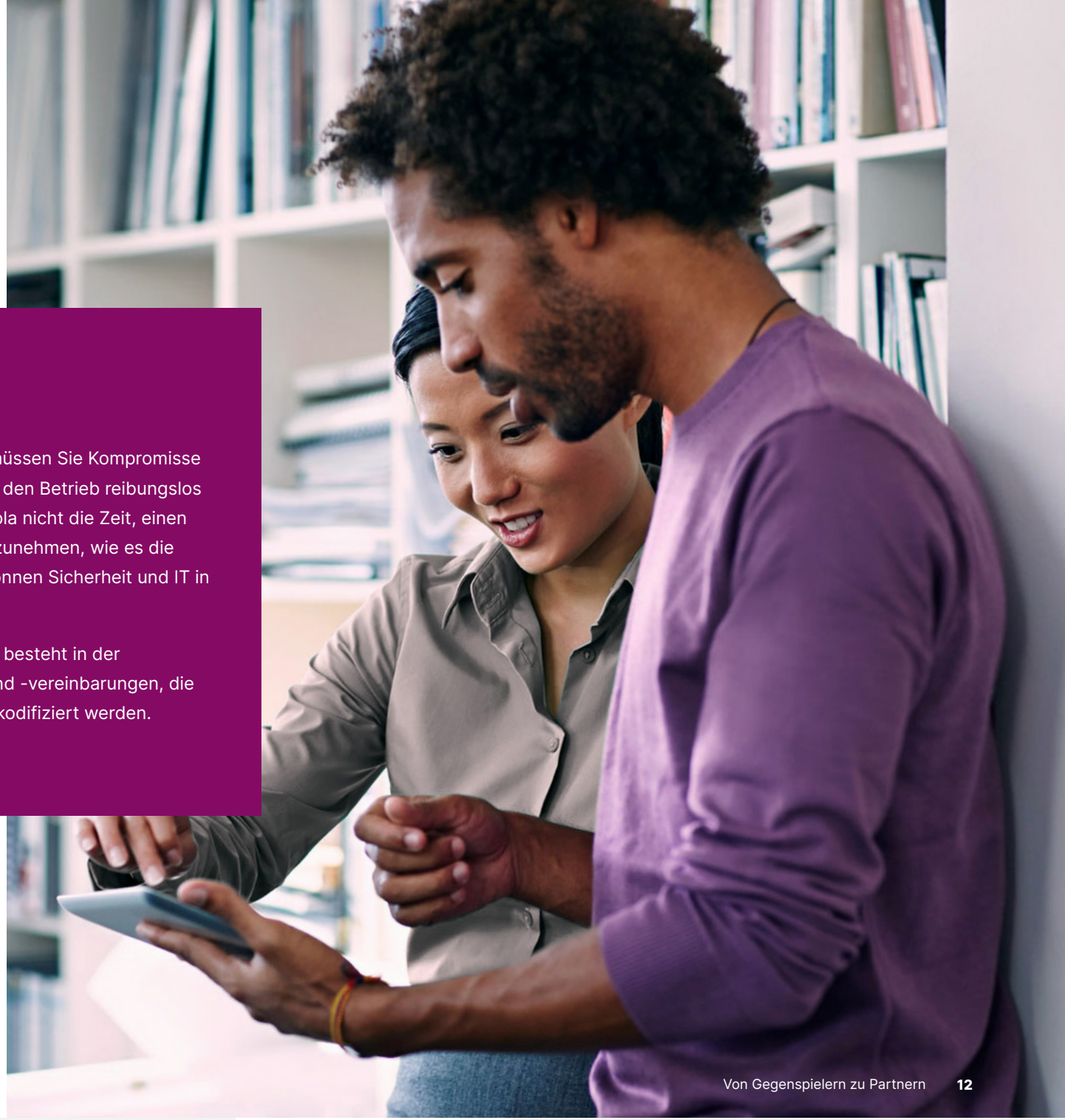
03

Kompromisse eingehen!

Verhalten Sie sich flexibel, wo Sie können, damit Sie nicht die „Abteilung der Neinsager" sind

ivanti

Der Stärke von Kompromissen



Wenn Sie mit einer anderen Abteilung zusammenarbeiten, müssen Sie Kompromisse eingehen. Die Priorität Ihres IT-Teams liegt schließlich darin, den Betrieb reibungslos aufrechtzuerhalten. Möglicherweise haben sie in ihrem Zeitpla nicht die Zeit, einen Patch zu veröffentlichen oder eine Änderung so schnell vorzunehmen, wie es die Sicherheitsabteilung sich wünscht. Wenn man flexibel ist, können Sicherheit und IT in der Regel einen Mittelweg finden.

Eine der Möglichkeiten, diese Flexibilität proaktiv zu nutzen, besteht in der Festlegung von gegenseitig vereinbarten Servicefenstern und -vereinbarungen, die in der Regel in Form von Service-Level-Agreements (SLAs) kodifiziert werden.

In diesem SLA sollten die Erwartungen an die Zusammenarbeit und der Zeitrahmen für jeden Schritt festgelegt werden, damit jeder weiß, was wann und von wem erledigt wird:

Alle Definitionen. Sie müssen ihre Kommunikation klarer gestalten, als Sie denken - selbst wenn es um so etwas Grundlegendes geht wie das, was Ihr Unternehmen als „ausgenutzte Schwachstelle" ansieht!

Erforderliche Spezifikationen und Tech-Stack-Implementierungen für jede Phase eines gemeinsamen Abteilungsprozesses.

- Diese Prozesse können von der Einführung von Patches bis zur Implementierung neuer Richtlinien reichen

Priorisierungskriterien. Finden Sie heraus, was für die Sicherheitsabteilung ein Notfall ist gegenüber dem, was für die IT-Abteilung ein Notfall ist.

- Maßgeschneiderte interne Skalen, Rubriken und andere interne Bewertungsmethoden können helfen, diesen Teil des Prozesses zu standardisieren. Entwickeln Sie diese gemeinsam mit Ihrem IT-Team als Teil des SLA-Erstellungsprozesses!

Häufigkeit der Kommunikation bei gemeinsamen Projekten. Denken Sie zum Beispiel an die folgenden prozessbezogenen Fragen:

- Wann kann die IT-Abteilung damit rechnen, von der Sicherheitsabteilung über die spezifischen Patch-Rollouts für einen bestimmten Patch Tuesday informiert zu werden?
- Wann kann die Sicerheitsabteilung damit rechnen, von der IT-Abteilung über etwaige Probleme oder eine Bestätigung der erfolgreichen Patch-Einführung informiert zu werden?
- Wann kann eine offene Anfrage (von beiden Seiten) mangels Antwort geschlossen werden? Wann sollten Vorgesetzte in die Kommunikation einbezogen werden?

„Standard"-Zeitpläne und Erwartungen an die Ergebnisse für jede Art von Projekt, von jedem Team - sowie ausdrücklich aufgeführte und beschriebene Ausnahmen vom Standardverfahren!

Benennung von Ansprechpartnern bzw. Ansprechpartnerinnen oder spezifischen Positionen in jeder Abteilung.

- Zu ihren Aufgaben gehört es, Unklarheiten über SLA-Richtlinien und -Verfahren zu beseitigen und die SLA jährlich mit ihren abteilungsübergreifenden Ansprechpartnern bzw. Ansprechpartnerinnen zu überprüfen und zu aktualisieren.

04

Entwickeln und Durchsetzen gemeinsamer Ziele mit dem IT-Team.

ivanti

Festlegen von gemeinsamen Zielen

Wie gesagt, haben Sicherheit und IT zwar unterschiedliche Ansätze, aber ähnliche Aufgaben: das Unternehmen, ihre User und alle Prozesse so reibungslos wie möglich zu gestalten.

Es lohnt sich daher, sich die Zeit zu nehmen, um diese gemeinsamen Ziele mit der IT-Leitung festzulegen - und auch, um Leistungsindikatoren (KPIs), Dashboards und andere gemeinsame Messungen zu erstellen, um die gemeinsamen Ziele auf taktischer, täglicher Basis zu stärken.

Denken Sie zum Beispiel die Einführung von Patches. (Das ist ein häufiges Beispiel in diesem eBook, aber aus gutem Grund!)

Sowohl IT- als auch Sicherheitsteams wollen, dass die Technologie eines Unternehmens reibungslos funktioniert. Beide Abteilungen wollen also nicht, dass ein Patch den Arbeitsablauf unterbricht, wenn auch aus unterschiedlichen Gründen:

- Die IT-Abteilung möchte sich nicht mit all den Helpdesk-Tickets befassen, die durch eine mangelhafte Patch-Implementierung entstehen, die den Usern oder die Konnektivität einer Anwendung beeinträchtigt.

- Die Sicherheitsabteilung möchte die User nicht verärgern und sie nicht dazu ermutigen, nach riskanten Umgehungslösungen und Schatten-IT-Implementierungen zu suchen, um ihre Arbeit zu erledigen, wenn eine (sicherere) gepatchte Unternehmensanwendung ihre zuvor etablierten Arbeitsabläufe aktiv beeinträchtigt.

Das gemeinsame Durchsetzen von Zielen verhindert Probleme

Gelegentlich besteht die Lösung des IT-Teams darin, Patches einfach gar nicht durchzuführen - vor allem, wenn die Sicherheitsabteilung nicht garantieren kann, dass ein Patch keine geschäftskritischen Arbeitsabläufe unterbricht. Außerdem kann es sein, dass die Sicherheitsteams angesichts des Widerstands der IT-Abteilung die Einführung von Patches vergessen.

Sowohl die IT-Abteilung als auch die die Sicherheitsabteilung möchten jedoch vermeiden, dass es zu einem Sicherheitsverstoß kommt - was häufig der Fall ist, wenn Geräte und Anwendungen nicht regelmäßig gegen aktive Sicherheitslücken aktualisiert werden.

Die Abwehr von Cyberangriffen liegt zwar eher in der Verantwortung und Last der Sicherheitsabteilung, aber auch das IT-Team leidet unter einer Sicherheitsverletzung.

Schließlich ist es die IT-Abteilung, die die technischen Systeme so schnell wie möglich wiederherstellen muss, während das Sicherheitsteam dafür sorgt, dass das Backup sicher ist und alle Eindringlinge aus dem Netzwerk entfernt werden.

Was wird von der Prioritätenliste der IT-Abteilung gestrichen, wenn ein Angriff erfolgt, der durch ein nicht gepatchtes System ausgelöst wird?

Es liegt also sowohl im Interesse der Sicherheits- als auch der IT-Abteilung, eine robuste Patching-Strategie zu entwickeln, die für beide Teams funktioniert – und das alles mit dem gemeinsamen Grundverständnis, dass beide Teams eine Unterbrechung der Unternehmensprozesse um jeden Preis vermeiden wollen.

Hilfe anbieten:

Teilen Sie proaktiv Ihre eigenen Verwaltungsressourcen, Ihr technisches Fachwissen und andere Tools.

Geben und Nehmen von beiden Seiten sorgt für eine bessere Zusammenarbeit

Wenn Sie etwas von der IT-Abteilung verlangen - z. B. die Übernahme und Anpassung ihrer aktuellen IT-Technologien, Richtlinien und Prozesse für Ihre eigenen Sicherheitsanwendungen -, dann müssen Sie im Gegenzug auch etwas zurückgeben.

Dazu gehört auch, dass die finanzielle Verantwortung für gemeinsam genutzte Tools und Unternehmen geteilt wird - wobei jedes Team einen geringeren Teil seines Budgets für das gemeinsame Tool aufwendet, als es für die Ressourcen jedes einzelnen Teams kosten würde -, aber diese Hilfe kann viele Formen annehmen.

Letztlich können Sicherheits- und IT-Teams durch die gemeinsame Nutzung von Tools und Ressourcen ihre Gesamtkosten senken und die Zusammenarbeit verbessern.

Gemeinsame Tools, Dashboards und Berichte schaffen einen Kontext, in dem sich beide Teams gegenseitig verstehen können. Diese Einblicke in die Welt des jeweils anderen schaffen Verständnis und Vertrauen.

Wenn die Sicherheitsteams die Werte und Prioritäten der IT-Abteilung kennen, können sie die Zustimmung zu verschiedenen Projekten auf eine Art und Weise gewinnen, die für ihre IT-Partner praktikabel ist und ihnen entgegenkommt.

Und diese Akzeptanz tritt noch schneller ein, wenn das Sicherheitsteam auf dem Weg Hilfe anbietet - natürlich in einem angemessenen Rahmen.

3 kreative Wege, wie das Sicherheitsteam dem IT-Team abgesehen von den Budgets helfen kann

Verbesserung im Verwaltungsbereich	Viele Menschen - auch Mitglieder von IT-Teams - finden den Papierkram in ihrem Job lästig. Wenn es dazu beiträgt, dass die andere Abteilung eine bessere Meinung von Ihnen hat, dann bieten Sie an, ihnen dies abzunehmen, soweit es Ihnen möglich ist. Wenn Ihr IT-Team beispielsweise prognostiziert, dass sich eine neue Sicherheitsrichtlinie auf die Warteschlangen auswirken wird, dann ernennen Sie einen Sicherheitsspezialisten, der alle Tickets und Benutzeranfragen im Zusammenhang mit der neuen Richtlinie beantwortet. Sie könnten die neue Richtlinie auch für ein nichttechnisches Publikum aus dem ursprünglich angenommenen Vorschlag „übersetzen“ und sie dann Ihrem internen Kommunikationsteam zur Weitergabe an die internen Stakeholder übergeben.
Technisches Fachwissen	Vielleicht schlagen Sie einen neuen Prozess oder eine neue Richtlinie vor, die Ihnen verständlich erscheint, Ihre IT-Ansprechpartner aber nicht verstehen. Bieten Sie dem zuständigen IT-Personal an, eine Schulung zu den taktischen Implementierungen durchzuführen. Wenn Sie Zeit haben, können Sie die Einstellungen auch im Auftrag der IT-Abteilung vornehmen. (Sorgen Sie dafür, dass die für die Wartung verantwortlichen IT-Mitarbeitenden alle relevanten Materialien zur Fehlerbehebung problemlos finden können!) Bitten Sie im Gegenzug die IT-Administratoren, das Sicherheitsteam zu schulen, damit es ein grundlegendes Verständnis dafür hat, wie die IT in Ihrem Unternehmen funktioniert - selbst wenn sie vom IT-Team selbst zum Sicherheitsteam gekommen sind!
Gemeinsame Ressourcen	In einem anderen Leitfaden gehen wir darauf ein, wie die Sicherheitsabteilung die Nutzung der technischen Möglichkeiten der IT-Abteilung verlangen kann. (Siehe „Shift-Left der Sicherheit“ für weitere Einzelheiten!) Es gibt jedoch keinen Grund, warum Sie dem IT-Team bestimmte sicherheitsrelevante Tools nicht nicht zur Verfügung stellen könnten - insbesondere den Zugang zu Weiterbildungs- oder Schulungsmaterialien, die Sie für Ihr eigenes Team bereithalten. Dadurch wird das Verständnis der IT-Abteilung für den Auftrag und die Position der Sicherheitsabteilung verbessert, was Ihnen helfen kann, künftige Anfragen an ihr Team zu beschleunigen.

Auswirkungen auf die reale Welt

Abteilungsübergreifendes „Ausschwärmen“ von Out-of-Band-Sicherheitsrisiken

Sowohl Sicherheits- als auch IT-Teams planen ihren Monat oft um die regelmäßigen monatlichen „Patch Tuesday“-Veröffentlichungen herum, indem sie einen festen Zeitplan für Tests, Pilotprojekte und Rollouts erstellen und methodisch alle Implementierungsprobleme angehen.

Einige Patches fallen jedoch „aus dem Rahmen”, sodass alle aus zwei Gründen nervös werden.

1. **Out-of-band-Patches oder Freigaben für Abhilemaßnahmen sind in der Regel aktive Exploits, die** sofort implementiert werden müssen.

2. Die**Teams müssen andere kritische Aufgaben zurückstellen ,** um dem neuen Risiko Vorrang zu geben - Aufgaben, die weiterhin Probleme verursachen, während der Notfall behoben wird.

Anstatt für solche Notfälle alle Mitarbeitenden einzuspannen, haben ausgereifte Unternehmen eine „Schwarmmethode“ entwickelt.

- Sie ernennen ein **spezielles Out-of-Band-Reaktionsteam** mit Experten aus verschiedenen Abteilungen, einschließlich Sicherheit und IT.
- Wenn ein Out-of-Band-Patch veröffentlicht wird, **„schwärmen“ diese Teams** um den Notfall-Patch oder die Abhilfemaßnahme herum und konzentrieren sich voll und ganz auf den Fix.
- In der Zwischenzeit **setzen** die übergeordneten Abteilungen **ihre regulären** Aufgaben und Projekte **fort** .

Indem diese funktionsübergreifenden Teams gebildet werden, bevor Out-of-Band-Patches auf den Markt kommen, können Unternehmen planmäßig weiterarbeiten und gleichzeitig schnell auf unvermeidliche Notfälle reagieren.

„Dies ist ein Kulturwandel, eine Schwarmmentalität.

Bei der Behandlung von Out-of-Band-Risiken versuchen wir nicht, den Schuldigen zu finden. In den meisten dieser Fälle ist eine Schwachstelle nicht die Schuld einer Person im Unternehmen.

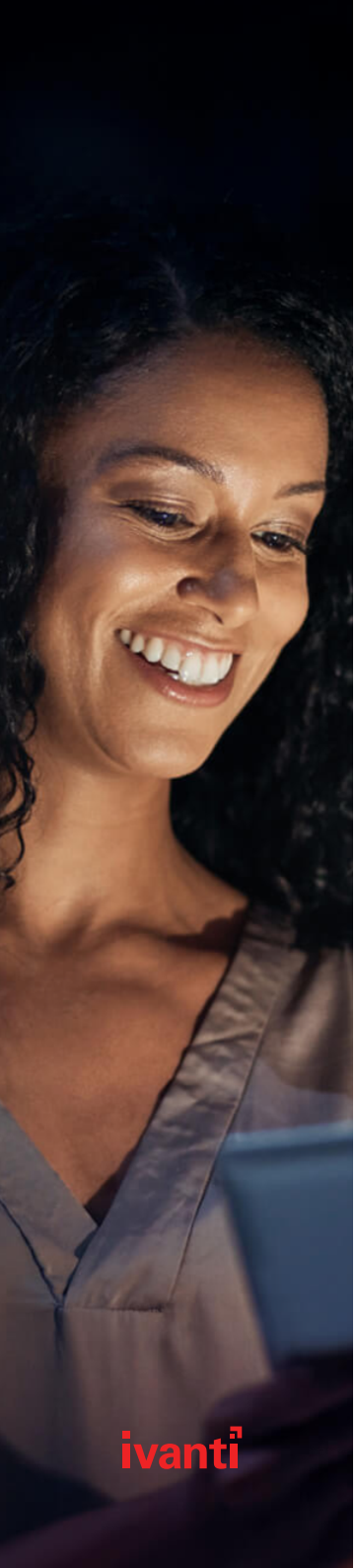
Stattdessen müssen wir in einer Schwarm-Situation einfach herausfinden, wer das Problem am besten lösen kann.

Jetzt, da wir diese Person identifiziert haben, wissen alle anderen im Unternehmen, dass, wenn sie diese Person bei der Arbeit unterstützen sollen, dies [Abhilfe] ihre neue Priorität ist.

Alle anderen Prioritäten verlagern sich nach unten, bis das Problem gelöst ist.

Die Unternehmen, bei denen ich gesehen habe, dass sie sich diese Schwarmmentalität zu eigen gemacht haben, reagieren besser und in der Regel schneller auf die Schwachstelle.“

- Chris Goettl
VP of Endpoint Security Product Management, Ivanti



Referenzen

- Australian Cyber Security Centre. (30 June 2017). “Essential 8 Maturity Model”: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Bowermaster, P. (February 2023). “Shift Left to Risk-Based Proactive Security Management.” CIO’s The Future of Work Summit.
- Center for Internet Security. (2021). “Critical Security Controls Version 8”: https://www.cisecurity.org/controls/v8
- Forrester. (2022). “The Total Economic Impact of Ivanti Unified Endpoint Management (UEM) Solutions”: https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf
- Forrester. (2022). “The Total Economic Impact of the Ivanti Enterprise Service Management. A Forrester Total Economic Impact Study Commissioned by Ivanti”: https://rs.ivanti.com/reports/forrester-tei-ivanti-enterprise-service-management-platform-2021.pdf
- GDPR.EU. (n.d.) “GDPR Checklist for Data Controllers”: https://gdpr.eu/checklist
- Goettl, C. (25 March 2021). “Automated Patch Management and Team Swarming are Key Security Practices.” Ivanti: https://www.ivanti.com/blog/automated-patch-management-and-team-swarming-are-key-security-practices
- Goettl, C., & Masserini, J. (1 September 2022). “Vulnerability Management in Real Life: 5 Best Practices from Real-World RBVM Programs.” Ivanti: https://www.ivanti.com/webinars/2022/vulnerability-management-irl-5-best-practices-from-real-world-rbvm-programs
- Goettle, C. & Stryker, A. (11 May 2023). “Vulnerability Patch Prioritization Problems: Cybersecurity Research Results Part 2.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12876518-vulnerability-patch-prioritization-problems-cybersecurity-research-results-part-two
- Harvard Business Review. (29 August 2022). “How Much Time and Energy Do We Waste Toggling Between Applications?”: https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications
- Ivanti. (18 August 2018). “7 Experts on What Shift Left Means for IT Departments”: https://www.ivanti.com/blog/7-experts-on-what-shift-left-means-for-it-departments
- Ivanti. (2022). “The NIST Cybersecurity Framework (CSF): Mapping Ivanti’s Solutions to CSF Controls”: https://www.ivanti.com/resources/v/doc/ivi/2694/63935da433e2
- Ivanti. (2022). “The Ultimate Guide to Risk-Based Patch Management”: https://www.ivanti.com/resources/v/doc/ivi/2705/11190ce11e80
- Ivanti. (2023). “Press Reset: A 2023 Cybersecurity Status Report”: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
- Ivanti. (2023). “ITSM+ Toolkit”: https://www.ivanti.com/resources/v/doc/ivi/2760/e094c24df239

Referenzen

- Ivanti. (2023). “The Ultimate Guide to Unified Endpoint Management (UEM)”: https://www.ivanti.com/resources/v/doc/ivi/2508/b7d55619d0ee
- Ivanti. (28 June 2022). “2022 Digital Employee Experience Report”: https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf
- Ivanti. (n.d.) “IT Jargon Explained: CMDB:” https://www.ivanti.com/glossary/cmdb
- Ivanti. (n.d.) “IESO Shifts Left for Streamlined IT Operations”: https://www.ivanti.com/customers/ieso
- Ivanti. (n.d.) “Southstar Bank “Shifts Left” with Ivanti Neurons”: https://www.ivanti.com/customers/southstar-bank
- Miller, T., & Spicer, D., Stryker, A. (19 January 2023). “IT vs Security: When Hackers Patch for Profit.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12071546-it-vs-security-when-hackers-patch-for-profit
- Morning Consult and IBM. (3 October 2022). “IBM Security Incident Responder Study”: https://www.ibm.com/downloads/cas/XKOY5OLO
- National Institute of Standards and Technology. (2018). “Framework for Improving Critical Infrastructure Cybersecurity” (p14): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Official Journal of the European Union. (14 December 2022). “Directive (EU) 2022/2555 of the European Parliament and of the Council”: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Oltsik, J. (2022). “ESG Research Report: Technology Perspectives from Cybersecurity Professionals.” Enterprise Strategy Group - Information Systems Security Association International: https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf
- Perri, L. (2023, April 19). “Top Strategic Cybersecurity Trends for 2023.” Gartner: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Pickering, D. (2022, May 5). “What is DevSecOps? How Great Developers Shift Left for Security.” Ivanti: https://www.ivanti.com/blog/what-is-devsecops-how-great-developers-shift-left-for-security
- Rundle, J. and Nash, K. (2023, May 22). “Security Chiefs Trim the Fat.” The Wall Street Journal: https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99
- SAM. (July 2022). “IoT Security Landscape Report”: https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf
  Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security
- Verma, A., Goettl, C., & Hindman, M. (2022). “How to Win Budget and Influence Non-InfoSec Stakeholders for Your 2023 Cybersecurity Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program

Von Gegenspielern zu Partnern

5 Möglichkeiten, Ihr Sicherheitsteam mit dem IT-Team zusammenzubringen

ivanti

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