
ivanti
Shift-Left der Sicherheit
Wie man reaktionsfähige Sicherheitsumgebungen mit aktuellen IT-Tools betreibt

Inhalt:

ivanti

01

Scheideweg der Sicherheit

Zwischen proaktivem Cybersicherheitsbedarf und technischem Konsolidierungsdruck abwägen

In diesem Abschnitt:

1. Schaffen eines reaktionsfähigen Cybersicherheitsökosystems...
2. ...oder Konsolidieren Ihrer Technologie-Stacks?
3. Wie Sicherheit beides auf einmal bieten kann!

ivanti

Am Scheideweg zwischen widersprüchlichen Sicherheitsaufgaben

Ihr Cybersicherheitsteam muss proaktiv handeln, um künftigen Risiken durch Cyberangriffe entgegenzuwirken und gleichzeitig aktuelle Sicherheitsmängel zu beheben. Das ist selbst für gut ausgestattete und unterstützende Unternehmen eine Mammutaufgabe, wenn sie gleichzeitig versuchen, ihren technischen Fußabdruck zu verkleinern und mit "weniger auszukommen", um dem erhöhten Budgetdruck in allen Abteilungen gerecht zu werden.

Wie können Sie beides erreichen?

Das ist natürlich der Grund, warum Sie diesen Leitfaden lesen – lassen Sie uns also beide Aufgaben im Kontext des breiteren Unternehmens betrachten.

Schließlich kann man nicht nur eine der beiden Herausforderungen angehen und die andere einfach ignorieren.

Ihr Sicherheitsteam muss einen Weg finden, sich um beides zu kümmern, um proaktiv und mit weniger Ressourcen Abhilfe zu schaffen.

Dieser Leitfaden gibt Ihnen praktischen Tipps.

Sicherheitsaufgabe Nr. 1:

Schaffen "reaktionsfähiger Cyber-Ökosysteme" für proaktive Abhilfemaßnahmen

In einem kürzlich erschienenen Gartner-Report beschreiben die Analysten beispielsweise, dass moderne Sicherheitsteams unbedingt ein "reaktionsfähiges Cyber-Ökosystem" entwickeln müssen.

Diese reaktionsfähigen Ökosysteme:

Scannen ununterbrochen die Umgebung

Identifizieren aktuelle und potenzielle Risiken

Versuchen zu reagieren, bevor Probleme auftauchen

Diese Ziele werden durch kontinuierliches Management der Bedrohungslage, Benutzer- und Zugriffsvalidierung und die Schaffung eines "digitalen Immunsystems" erreicht, das Sicherheitslücken erkennt und minimiert.

Dies sind ehrgeizige Maßnahmen für jedes Sicherheitsteam, aber besonders schwierig in der heutigen Umgebung, die auf die Reduzierung von Sicherheitstools ausgerichtet ist – wie wir weiter unten besprechen werden.

ivanti

Diese Trends begünstigen die Bemühungen zur Risikobewältigung, indem sie einen **kontinuierlichen Ansatz für das Bedrohungsmanagement und die Validierung der Cybersicherheit** anwenden. Sie tragen dazu bei, die Erkennungs- und Reaktionsmöglichkeiten zu verbessern und digital immunere Identitätsökosysteme aufzubauen.

- Gartner
"Die wichtigsten strategischen Trends im Bereich der Cybersicherheit für 2023"
Gartner

Sicherheitsaufgabe Nr. 2:

Konsolidieren der Tech-Stacks in den Sicherheitskostenstellen

Der zweite Trend zur Konsolidierung und Umstrukturierung von Sicherheitstools verdeutlicht, dass sich selbst Sicherheits- und IT-Abteilungen dem finanziellen Druck einer unberechenbaren Wirtschaft nicht vollständig entziehen können.

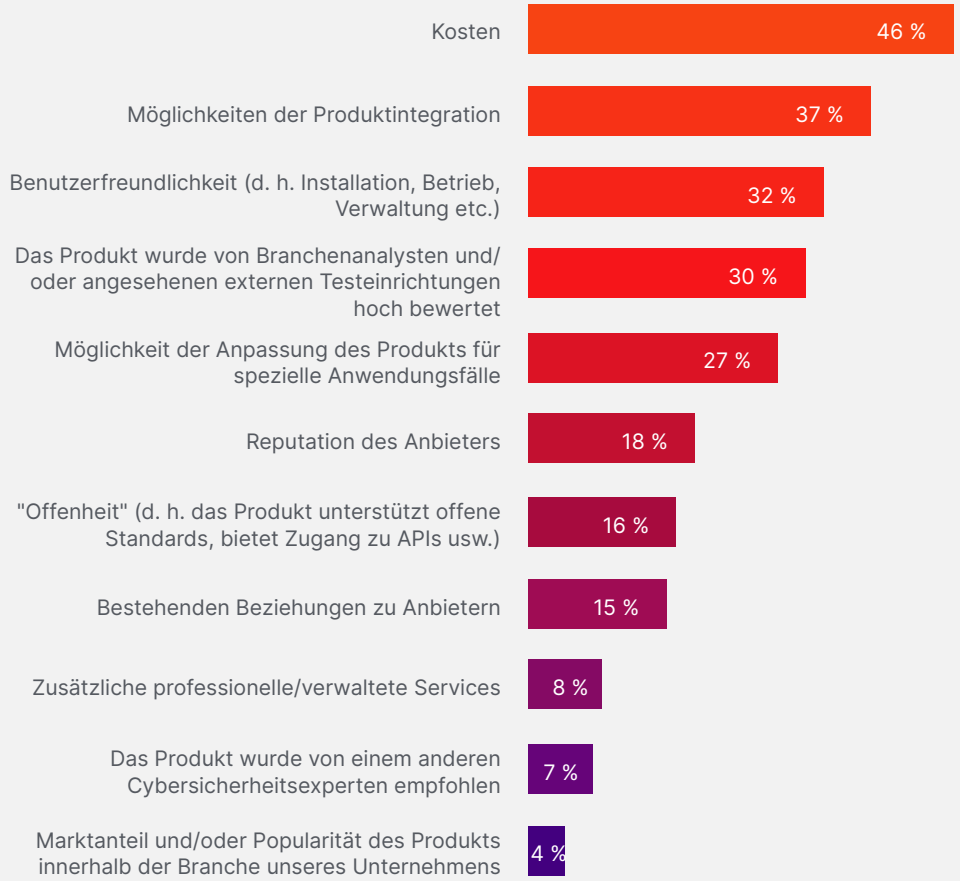
Denn beide Teams sind zwar wichtig für die Sicherheit und das Funktionieren des Unternehmens, generieren aber keinen direkten Umsatz.

Diese Wahrnehmung von Sicherheit als Kostenstelle hat zu einem erhöhten Druck auf CSOs und CISOs geführt, die Gemeinkosten der Abteilungen zu senken – zum Teil durch Technologiekonsolidierung und verstärkte Integration ihrer aktuellen Tools – laut Brancheninterviews des Wall Street Journal.

Und laut einer aktuellen Studie von ESG und ISSA achten die befragten Cybersicherheitsexperten eher auf Kosten, Produktintegrationsmöglichkeiten und Benutzerfreundlichkeit als auf Tests Dritter oder Empfehlungen von Branchenanalysten.

Dieser Druck hat Unternehmen dazu gedrängt, ihre Tech-Stacks zu konsolidieren und multifunktionale Plattformen anstelle von Nischen- oder "Best-of-Breed"-Technologien einzusetzen.

Welche der folgenden Produktüberlegungen sind für Ihr Unternehmen beim Kauf von Cybersicherheitstechnologien am wichtigsten?



(Prozentualer Anteil der Befragten, N=280, drei Antworten möglich) Quelle: ESG, ein Bereich von TechTarget, Inc.

Der dritte Weg: Nutzen von abteilungsübergreifenden Tools für proaktive Sicherheitsanwendungen

Mit zwei scheinbar gegensätzlichen Aufträgen – nicht nur aktuelle, sondern auch künftige kritische Probleme zu lösen – und mit einem zunehmend begrenzten Budget, in dem kein Platz für Einweg-Tools ist, stehen Sicherheitsteams vor einer unmöglichen Entscheidung an einem unklaren Scheideweg.

Welchen Weg sollen sie einschlagen?
Welche Priorität steht für sie an erster Stelle?

Aber was wäre, wenn es einen neuen Weg gäbe: einen noch unbenannten dritten Weg, der es den Sicherheitsteams ermöglichen würde, beide Anforderungen zu erfüllen?

Diese dritte Option muss zu beiden Ergebnissen führen – proaktive Abhilfemaßnahmen und weniger teure punktuelle Tools – ohne sich in der Umsetzung zu verlieren, Teams zu überfordern oder Zeit und Ressourcen zu verschwenden.

Dieser Weg ist nur möglich, wenn die Sicherheitsteams die Tools und Lösungen anderer Teams für ihre eigenen Anwendungsfälle besser wiederverwenden und zu einem anderen Zweck nutzen können.

Die erste Gelegenheit? Die aktuellen Tools und Architekturen des IT-Teams.

Auf diese Weise können Sicherheitsteams eine reaktionsschnelle Cybersicherheitsumgebung schaffen und gleichzeitig die Kosten durch die Wiederverwendung bereits etatisierter und genutzter IT-Plattformen senken.

Und die Vorteile des Sicherheitsteams, das bereits implementierte IT-Tools nutzt, gehen über unmittelbare Kosteneinsparungen hinaus. Analysten sind sich einig, dass die Vereinfachung von Tools häufig die Abläufe verbessert und die Effizienz der Mitarbeitenden erhöht.

Gemeinsame Tool-Plattformen erreichen außerdem:

- Verstärkung der abteilungsübergreifenden Zusammenarbeit,
- Verringerung des Verwaltungsaufwands für jedes einzelne Team und
- Verbesserung der allgemeinen Cybersicherheitslage.

Es ist also möglich, dass Sicherheitsteams taktisch proaktive Abhilfemaßnahmen durchführen, ohne dass die Nischen-Tools auf einen einzigen Anwendungsfall ausgerichtet sind – aber nur, wenn sich Sicherheits- und IT-Teams gemeinsam auf die Bedeutung des "Shift-Left" über die Reduzierung von IT-Helpdesk-Tickets oder DevSecOps-Anwendungen der Sicherheit hinaus verständigen.

02

Definition des "Shift-Left" über DevSecOps hinaus:

Eine gemeinsame Definition verbindet Sicherheits- und IT-Ansätze

In diesem Abschnitt:

1. Widersprüchliche Definitionen des "Shift-Left" der Sicherheit und IT
2. Ein gemeinsamer Ansatz für den "Shift-Left“

ivanti

Widersprüchliche Definitionen des "Shift-Left" der Sicherheit und IT

Sowohl in der Sicherheits- als auch in der IT-Branche wird der Begriff "Shift-Left“ verwendet, aber jedes Team definiert den Begriff anders. Diese Unterschiede führen trotz einiger Gemeinsamkeiten und gemeinsamer Ziele zu größeren Reibungen zwischen den Teams.

Definition des "Shift-Left"		Das "Shift-Left" der IT bei Helpdesk-Tickets
Definition	Sicherheitsspezialisten und -tools ermitteln Sicherheitsrisiken während der Entwicklung und nicht erst in letzter Minute vor der endgültigen Bereitstellung.	Die Technologie identifiziert automatisch potenzielle IT-Probleme, bevor Endbenutzer sie bemerken und Helpdesk-Tickets einreichen.
Fokus	Konzentriert sich auf die Produkt- und/oder Prozessentwicklung im Rahmen eines DevSecOps-Release-Modells.	Konzentriert sich auf das Servicemanagement von IT-Helpdesk-Verpflichtungen gegenüber internen Endbenutzern.
Unmittelbare Ergebnisse	Reduziert Verzögerungen bei der Produkt- und Prozessbereitstellung durch proaktive, kontinuierliche Abhilfemaßnahmen.	Reduziert die Gesamtzahl der Helpdesk-Tickets und senkt die Eskalationsrate an höherrangige IT-Spezialisten.
Sonstige Vorteile	Fördert eine Unternehmenskultur, bei der die Sicherheit an erster Stelle steht, da sie nicht mehr erst in letzter Minute berücksichtigt wird. Beseitigt Silos, da die Sicherheit vom externen Regulierer zum integralen Teammitglied verlagert wird.	Befähigt weniger spezialisierte IT-Experten, Probleme zu beheben. Geringere Gesamtarbeitskosten durch weniger Bedarf an Help-Tickets.
Zeitleiste Auswirkungen	Die IT-Abteilung sollte die Sicherheitsabteilung von Beginn an proaktiv einbinden und nicht bis zum Ende eines Projekts warten. So werden Verzögerungen durch zu spät geäußerte Bedenken verhindert. Entwicklungszeiten für Produkte und Prozesse werden zunehmend vorhersehbarer (wenn auch möglicherweise länger) und die bekannten Sicherheitsrisiken reduziert.	Das IT-Personal hat nun Zeit und Ressourcen für die berufliche Weiterbildung und mehr Kapazität für strategische, proaktive Aufgaben.

So unterschiedlich die taktischen Ausprägungen des Shift-Left für die Sicherheits- und IT-Teams auch sind, so haben die Anwendungsfälle der beiden Abteilungen doch einige grundlegende Gemeinsamkeiten.

In der Tat zeigen beide Modelle, dass Sicherheit und IT ein gemeinsames Bedürfnis nach proaktiven, weniger zeitintensiven Abhilfemaßnahmen in einem frühen Stadium des Prozesses haben, um kostspielige Notfälle in letzter Minute zu vermeiden.

Ein gemeinsamer Ansatz des "Shift-Left“ der Sicherheit und IT

Bei Ivanti verwenden wir den Begriff "Shift-Left“ für jeden strategischen Prozess, der Probleme deeskaliert und behebt, bevor sie zu echten Problemen oder Notfällen werden – oft bevor externe Stakeholder merken, dass es überhaupt ein Problem gibt!

Auf diese Weise wird das Shift-Left zu einem kulturellen Ansatz der automatischen, proaktiven Abhilfe, der abteilungsübergreifend ist und zuvor getrennte Prozesse unter einem einzigen, einheitlichen Grundansatz vereint.

Diese Definition spiegelt zwar den Hauptanwendungsfall der IT wider – d. h. die Behebung von Problemen, bevor sie auftreten und bevor irgendjemand sonst weiß, dass es ein Problem gibt –, aber dieser Shift-Left-Ansatz orientiert sich eng an dem Auftrag der Sicherheitsabteilung, ein proaktives und reaktionsfähiges Ökosystem zu schaffen, das über DevSecOp-spezifische Implementierungen oder Überlegungen hinausgeht.

Probleme zu beheben, bevor Menschen sie bemerken, spielt die Automatisierung eine wichtige Rolle bei der Unterstützung jeder Abteilung im Rahmen der Umstellung auf Shift-Left – besonders aber bei gemeinsamen Sicherheits- und IT-Anwendungsfällen.

Was bedeutet Shift-Left?

In diesem Leitfaden beziehen wir uns auf die strategischen Prozesse und taktischen Automatisierungen, mit denen **kleinere Probleme erkannt, deeskaliert und behoben werden können, bevor sie sich zu größeren Notfällen entwickeln –** meistens, bevor externe Stakeholder überhaupt von der Existenz von Problemen erfahren.

03

IT-Tools + Sicherheit

Praktische Anwendungsfälle für Sicherheitsteams, um vorhandene IT-Tools bedarfsgerecht zu nutzen

In diesem Abschnitt:

1. ITAM und ITSM + Sicherheit
2. UEM + Sicherheit

ivanti

Gemeinsame IT-Tools für die Sicherheit: ITAM, ITSM und UEM

Von allen möglichen IT-Tools, die für die Sicherheit genutzt werden können, konzentrieren wir uns auf zwei gängige Lösungsplattformen: Service-Management sowie Geräte- und Endpunktmanagement

Diese Lösungen können weiter in drei verschiedene Tools unterteilt werden:

1. IT-Asset-Management (ITAM).
2. IT-Service-Management (ITSM).
3. Unified Endpoint Management (UEM), das auch moderne Gerätemanagement-Clients und -Funktionen (MDM) umfasst.

Obwohl die IT-Abteilung traditionell die Überwachung und die Budgetierung für diese gemeinsamen Technologien innehatte, kann der Sicherheitsbereich dennoch mit seinen IT-Partnern zusammenarbeiten.

Diese Partnerschaft macht aus einer einmaligen Lösung und einem Nischenprodukt-Stack eine robuste, abteilungsübergreifende Mehrzweckplattform, die Konsolidierungsmaßnahmen überstehen kann.

Gemeinsame IT-Lösungen und -Tools

Service-Management

ITAM (IT-Asset-Management)

- Automatisch aktualisierte Liste/Datenbank der Assets eines Unternehmens
- Kann Standard- und Standardvariablen über Assets, Benutzer und Aktivitäten verfolgen

ITSM (IT-Service-Management)

- Zentrales Benutzer-Job-Board und Quasi-Projektmanager der IT
- Kann Wikis, FAQs und interne Formularfunktionen enthalten
- Kann IT-bezogene Backend-Automatisierungen hosten

Geräte- und Endpunktmanagement

UEM (Unified Endpoint Management)

- Grundlegendes Endgerätemanagement und Richtlinienkontrolle
- Kann MDM-Clients enthalten, die auf jedem Gerät und Endpunkt des Unternehmens vorhanden sind

ITAM und ITSM + Sicherheit

In diesem Abschnitt:

- Definition von ITAM und ITSM
- Sicherheitsspezifische Anwendungsfälle von ITAM und ITSM
- Shift-Left der Sicherheit mit ITAM und ITSM

Kurze Definitionen: ITAM und ITSM

IT-Asset-Management-Tools (ITAM)	IT-Service-Management-Tools (ITSM)
ITAMs ermöglichen das Management von Konfigurationselementen (CIs), wie Hardware- und Software-Assets.	ITSM verbessert die Fähigkeit der IT-Abteilung, Technologieanfragen von Endbenutzern und anderen internen Kunden zu verfolgen, zu beantworten und zu bedienen.
Mit diesem Tool können Unternehmen CIs während ihres gesamten Lebenszyklus konfigurieren, optimieren und verfolgen – vom Kauf bis zur Entsorgung.	ITSMs können auch zusätzliche Funktionen enthalten, mit denen die Benutzer einfache und häufige technische Probleme im Sinne der "Selbsthilfe" beheben können, sodass der Helpdesk-Support auf ein Minimum reduziert wird.

ITAMs kommen selten ohne ITSM-Plattformen von Partnern vor, obwohl ITSM-Produkte ohne zusätzliche ITAM-Partnerfunktionen implementiert werden können.

Gemeinsam erfasst und trackt eine gute ITAM- und ITSM-Lösungsplattform Folgendes:

- Original-Kaufdatum und Informationen.
- Gerätebesitzer und -benutzer.
- Aktuell angewandte Richtlinien für den Benutzerzugriff auf Anwendungen.
- Software-Betriebssystem sowie aktuelle Anwendungs- und Softwareinstallationen und -nutzung.
- Gerätestandort
- Gerätetyp
- Leistung, Nutzung und Compliance-Status.

Sicherheitsspezifische Anwendungsfälle von ITAM und ITSM

Mit dem richtigen Aufbau, den richtigen Richtlinien und der richtigen Zusammenarbeit mit dem IT-Team können die aktuellen ITAM- und ITSM-Plattformen Ihres Unternehmens wichtige Erkenntnisse für Sicherheitsteams liefern, z. B:

1

Dynamische Asset-Erkennung

2

Möglichkeiten der Konfigurationsmanagement-Datenbank (CMDB)

3

Verbesserung im Bereich Governance, Risiko und Compliance (GRC)

4

Besondere IT-Automatisierungen, die neu konfiguriert werden können, um hochgradig manuelle Sicherheitsaufgaben zu unterstützen

1 Sicherheit und Asseterkennung

Asseterkennung und -verwaltung ist die Grundlage für jedes Sicherheitsprogramm. In der Tat betrachten alle wichtigen Frameworks für Cybersicherheit (CSF) oder Datenschutzvorschriften die Asseterkennung als grundlegend für den Aufbau eines sicheren Systems.

Warum? Nun, der erste Schritt zu einem erfolgreichen Cyberangriff ist in der Regel die Erkundung. Ein bösartiger Akteur möchte Einblick in die KE-Ressourcen und -Systeme eines Unternehmens erhalten, damit er weiß, was und wie er einen Angriff starten kann.

Anforderungen an die Asseterkennung in ausgewählten CSFs

CSF	Relevanter Abschnitt	Relevante Zitate für die Asseterkennung
NIST Cybersecurity Framework	Erste Kernfunktion: Identifizieren	"Identifizieren: Entwicklung eines organisatorischen Verständnisses für das Verwalten von Cybersicherheitsrisiken für Systeme, Menschen, Assets, Daten und Fähigkeiten".
Center for Internet Security (CIS) Kritische Sicherheitskontrollen, V8	Erste Kontrolle: Bestand	**"Aktive Verwaltung (Bestand, Nachverfolgung und Korrektur) aller Unternehmensassets** (Endbenutzergeräte, einschließlich tragbarer und mobiler Geräte, Netzwerkgeräte, Internet of Things (IoT-Geräte und Server), die mit der Infrastruktur verbunden sind – physisch, virtuell, aus der Ferne und in Cloud-Umgebungen –, um **die Gesamtheit der Ressourcen**, die im Unternehmen überwacht und geschützt werden müssen, genau zu **kennen**." "Dies unterstützt auch die **Identifizierung von nicht autorisierten und nicht verwalteten Assets**, die es zu entfernen oder zu bereinigen gilt."
Australia Cyber Security Centre: Essential Eight	Übersicht über die einzelnen Stadien	"Dieses System umfasst die Asseterkennung als einen wichtigen Schritt zur Verhinderung von Angriffen in jedem Stadium."
Europäisches Recht Richtlinie 2022/2555 (NIS2)	Paragraph 44	"Die CSIRTs [Computer Security Incident Response Teams] sollten in der Lage sein, auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die internetfähigen Assets des Unternehmens sowohl innerhalb als auch außerhalb der Geschäftsräume zu überwachen, um die allgemeinen organisatorischen Risiken des Unternehmens im Hinblick auf neu identifizierte Kompromittierungen der Lieferkette oder kritische Schwachstellen zu ermitteln, zu verstehen und zu verwalten."

Jedes Framework macht deutlich, dass Ihr Sicherheitsteam zur Abwehr von Cyberangriffen genau wissen muss, was Sie schützen.

In der Praxis haben die meisten Unternehmen tendenziell eine Lücke von 20-30 % in der Transparenz ihrer Netzwerkressourcen.

Tatsächlich geben nur 47 % der IT-Fachleute an, dass ihre Unternehmen vollen Einblick in jedes Gerät haben, das versucht, auf ihr Netzwerk zuzugreifen.

Die gleichen automatischen Funktionen zur Asseterkennung, die in verschiedenen IT-Technologieplattformen – einschließlich ITSM- und ITAM-Produkten – enthalten sind, könnten es den Sicherheitsteams jedoch ermöglichen, die mit technologischen Anlagen und Benutzern verbundenen Risiken proaktiv zu analysieren.

"Wenn wir nicht wissen, was in unserer Umgebung los ist, können wir sie nicht sichern.

"Das Wichtigste beim Schwachstellenmanagement **ist es, die Angriffsfläche zu kennen und zu wissen, was sichtbar ist**

- Chris Goettl
VP of Endpoint Security Product Management, Ivanti

Die IT-Abteilung kann durch die automatische Asseterkennung die geplanten Geräte- und Softwarekäufe mit den im Netzwerk vorhandenen Geräten und Nutzungsstatistiken abgleichen.

Bei einer Synchronisierung mit einem ITSM-System können diese Statistiken mit Helpdesk-Anfragen von Benutzern verknüpft werden, um IT-Tickets und mögliche Ausfälle in einen Zusammenhang zu setzen.

Für Sicherheitsteams können dieselben Funktionen zur Asseterkennung in den IT-Lösungen wiederverwendet werden, um die Anforderungen an die Bestandsermittlung eines beliebigen Sicherheits-Frameworks zu erfüllen..

Außerdem kann der Anwendungsfall der automatisierten Asseterkennung im Bereich Sicherheit noch weiter ausgedehnt werden, als es die Standardeinstellungen vermuten lassen, was den Sicherheitsteams hilft:

Das Gerät

eines Anbieters zu **erkennen** und den Zugriff zu kontrollieren, um die Zugriffsrichtlinien Dritter zu erfüllen,

Geräte

aus der Ferne auf die Einhaltung der Sicherheitsrichtlinien des Unternehmens und auf Patch-Updates zu **scannen**, und

Transiente Geräte

zu **segmentieren oder zu reparieren.**

2 Sicherheit und CMDB

Der erste und grundlegendste Schritt zu einer proaktiven Sicherheitsimplementierung ist die Kenntnis der eigenen Assets. Damit Ihr Team jedoch die gesamte Risikoumgebung Ihres Unternehmens vollständig verstehen kann, müssen Sie wissen, wie die einzelnen Geräte, Anwendungen und Benutzer miteinander interagieren.

Die Configuration Management Database (CMDB) der IT bietet einen wichtigen Einblick in diese Zusammenhänge.

Während ein ITAM den Lebenszyklus eines Assets verfolgt, verwalten CMDBs – die häufig in ITSM-Plattformen integriert sind – die Zusammenhänge zwischen Konfigurationselementen (CIs) und ihrer Umgebung.

Wie ein ITAM enthält eine CMDB grundlegende Asset- und Benutzerinformationen, z. B. wer eine bestimmte Workstation nutzt und wo sie sich befindet. Sie enthält aber auch kontextbezogene Informationen, z. B. darüber, welche Geräte und Software mit dieser Workstation interagieren.

Einem erfahrenen Sicherheitsexperten geben diese Beziehungen Aufschluss über das Risiko, dem ein Konfigurationselement ausgesetzt ist – und Hinweise darauf, wie dieses Risiko gemindert werden kann.

3 Sicherheit und GRC

Die Abbildung dieser netzinternen Beziehungen und Aktivitäten ermöglicht auch ein kontextbezogenes Echtzeitverständnis und die Durchsetzung von Governance, Risiko und Compliance (GRC).

Wie ITAMs und ITSMs die GRC der Sicherheit unterstützen

Governance

Größerer Kontext durch gemeinsame Daten
Niemand möchte eine Anweisung erteilen, die keiner befolgt – oder die für sein Team oder sein Unternehmen nicht relevant ist.

Sicherheits- und IT-Teams können den Führungskräften dabei helfen, die aktuelle Risiko-, Benutzer- und Assetumgebung ihres Unternehmens zu verstehen und mit Hilfe der von ITAM- und ITSM-Funktionen gesammelten genauen Daten relevante und sinnvolle Richtlinien zu formulieren.

Standardrichtlinien über Backends
Durch die Verwendung derselben Backend-Systeme, die die IT-Abteilung bereits verwaltet, können Sicherheitsteams sicherstellen, dass ihre sicherheitsorientierten Richtlinien, Kontrollen und Dokumentationen organisiert und leicht zugänglich sind.

Außerdem wird so gewährleistet dass die Richtlinien standardmäßig in die umfassendere organisatorische Dokumentation aufgenommen werden, die die Technologieprozesse in allen Abteilungen bestimmt.

Risiken

Abbildung der Angriffsfläche durch Erkennung
Mithilfe von ITSM- und ITAM-Produkten können Sicherheitsteams die potenzielle Angriffsfläche ihres Unternehmens abbilden und die Struktur von Netzwerk, Geräten und Benutzern analysieren.

Ein besseres Verständnis der tatsächlichen Angriffsfläche, die das Ziel von Hackern sein kann, gibt Aufschluss über die Sicherheitsstrategien und -taktiken, die am besten auf die einzigartige Bedrohungsumgebung und die Netzwerkaktivitäten des Unternehmens abgestimmt sind.

Automations-Trigger über CMDB
Sicherheitsteams können aktuelle CIs nutzen und benutzerdefinierte, sicherheitsspezifische Variablen erstellen, die in der CMDB des ITAM sowohl als Trigger als auch als Komponenten automatisierter Formeln verfolgt werden.

Compliance

Durchsetzung bei den Anbietern mittels Datenerhebung
Mithilfe von Daten, die über ITAM-Listen und sich ständig aktualisierende ITSM-Plattformen gesammelt werden, können Sicherheitsteams dazu beitragen, Anbieterverträge zu verfassen, die die Einhaltung der Unternehmensrichtlinien in der Praxis unterstützen und durchsetzen und so die Sicherheitsrisiken in der Lieferkette verringern.

Durchsetzung von Endpunktsicherheit mittels Erkennung
Die Asset-Erkennungsfunktionen ermöglichen es sowohl der IT- als auch der Sicherheitsabteilung, nicht autorisierte Geräte in sensiblen Unternehmensnetzwerken zu identifizieren.

Diese Funktionen könnten auch automatische Konformitätswarnungen für Geräte, Netzwerksegmentierung oder sogar eine vollständige Quarantäne von Endgeräten unterstützen, die über andere IT-Tools, wie UEM- und MDM-Clients, bereitgestellt und durchgesetzt werden.

Durchsetzung von Sicherheitsvorkehrungen mittels IT-Richtlinien
Dieselben IT-Funktionen, die allgemeine Computerrichtlinien im gesamten Unternehmen durchsetzen, können bei Bedarf auch über Sicherheitsprotokolle reporten und diese durchsetzen – vom Aufstellen von digitalen Leitplanken für IT-Administratoren, die Benutzer bei Helpdesk-Problemen unterstützen, bis hin zum Senden von Warnmeldungen über mögliche Richtlinienverstöße oder Hinweise auf Insider-Bedrohungen.

Praktische Auswirkungen

Ein Gedankenexperiment: Tablets in Krankenhäusern

Stellen Sie sich einen Moment lang vor, Sie arbeiten in einem Krankenhaus.

Ihre IT- und Sicherheitsteams überwachen alle internetfähigen Endgeräte, einschließlich Tablets, auf die nur medizinisches Personal Zugriff haben sollte.

Einem Sicherheitsspezialisten fallen jedoch einige merkwürdige Aktivitäten fürein Tablet auf, der eigentlich nur auf interne Krankenhausdatenbanken und Intranets zugreifen sollte.

Tatsächlich wurde protokolliert, dass das besagte Tablet Zugriff auf einen externen Internetbrowser hatte – und offenbar versucht wurde, "undichte" Spiele-Apps herunterzuladen.

Da dieses verdächtige Verhalten durch ITSM- / ITAM-Automatisierungen –zum Teil unter Verwendung von CMDB-Protokollen und CI-Variablen – erkannt wurde, untersucht Ihr Sicherheitsteam die Aktivitäten und befragt die zuletzt angemeldeten Benutzer dazu.

Schließlich gab der Vorgesetzte der Station zu, dass das Personal den Patienten inoffiziell erlaubte, das Tablet zum gelegentlichen Surfen im Internet zu nutzen, während sie behandelt wurden.

(In dieser Station werden nur pädiatrische Patienten behandelt!)

Zugegebenermaßen verstieß der Vorgesetzte gegen interne Protokolle und Richtlinien, die dazu dienen, alle – auch die Kinder! – vor Hackern zu schützen.

Das Sicherheitsteam kann jedoch beschließen, diesen fehlbaren Endbenutzer nicht zur Verantwortung zu ziehen, da es eher von guten Absichten als von Faulheit oder schlechtem Verhalten ausgeht.

Stattdessen kann das Sicherheitsteam mit der IT-Abteilung zusammenarbeiten und ältere, bald ausgemusterte Tablets für den Einsatz umfunktionieren.

Mit diesen Tablets könnten Patienten während der Behandlung (sicherheitsgeprüfte) Spiele spielen, während sie von den sensiblen Intranets des Krankenhauses abgeschirmt sind – und jede böswillige Aktivität wird automatisch verfolgt.

Auch wenn es anfangs allen Beteiligten ein wenig Mühe macht, wäre diese Lösung ein dreifacher Gewinn:

Die Patienten fühlen sich wie zuvor gut betreut und behandelt.

Die Sicherheits- und IT-Teams verhindern gemeinsam , dass sie zur "Abteilung des Neins" werden und eine Richtlinie durchsetzen, die die Benutzer aktiv versuchen zu umgehen.

Das Endbenutzerpersonal hat so eine bessere Möglichkeit, als ihre "echten" Tablets mit den Patienten zu teilen. Sie fühlen sich sicher und sind daher eher bereit, künftigen Sicherheits- und IT-Anforderungen gerecht zu werden.

4 Das "Shift-Left" des Workloads der Sicherheitsabteilung mit ITAM- und ITSM-Automatisierungen

Wenn Sie darüber nachdenken, die IT-Tools für Sicherheitsanwendungen zu übernehmen – insbesondere ITAM und ITSM –, sollten Sie überlegen, wie Sie die derzeitigen IT-orientierten Automatisierungen und Implementierungen nutzen können, um das Shift-Left Ihres Teams zu fördern.

Sie werden feststellen, dass Sie mit weniger Arbeitsaufwand mehr Sicherheitsmaßnahmen ergreifen können, die über einfache Warnungen und Anzeigen auf Dashboards hinausgehen und eine wirklich proaktive Risikobeseitigung ermöglichen.

1

Verbesserung der Self-Service-Optionen für Endbenutzer

mittels Sicherheitsanfragen und anderer die IT betreffenden Fragen, sodass Ihre leitenden Analysten von der Identifizierung von Phishing entlastet werden.

2

Vereinheitlichung der Lösung von Sicherheitsvorfällen

mittels der Ticketing-Software der IT-Abteilung und den Warteschlangen für die Priorisierung (die aus den Anfrageformularen abgerufen werden), um eine bessere Priorisierung, Nachverfolgung und Kontextualisierung zu ermöglichen.

3

Wiederverwendung von IT-Automatisierungen im Hintergrund

für Sicherheitszwecke, da dieselben Automatisierungen, die Geräte reparieren können, bevor Benutzer Tickets einreichen müssen, auch Endpunktumgebungen besser schützen und bösartige Aktivitäten erkennen können.

ivanti

Automatisierung Nr. 1:

Verbesserung des Sicherheits-Self-Service für "Level Zero"-Support.

Das gleiche System, das die IT-Helpdesks entlastet, kann auch für Sicherheitsfragen verwendet werden!

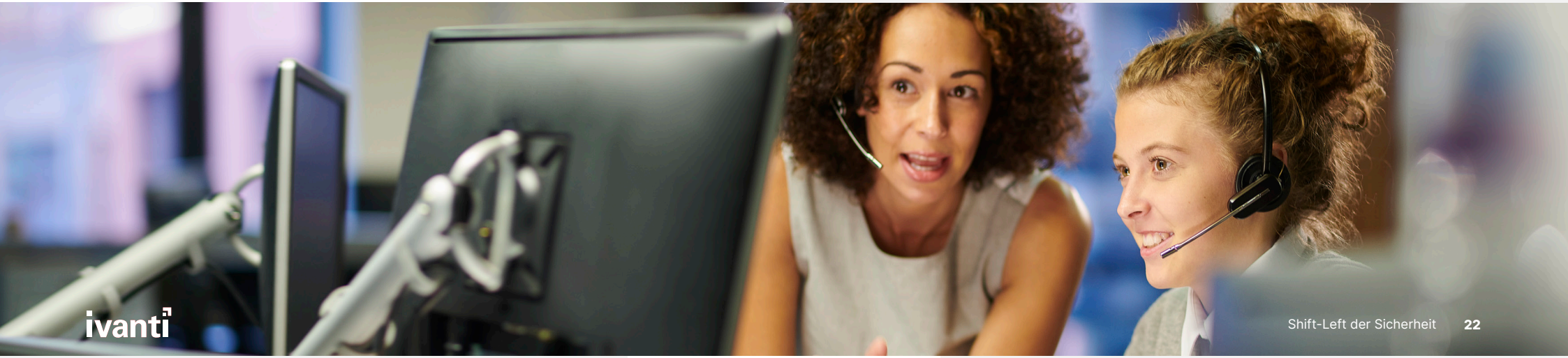
Durch die Zentralisierung allgemeiner sicherheitsrelevanter Fragen und Anfragen – wie z. B. die Aktivierung der Zwei-Faktor-Authentifizierung, die Meldung eines vermuteten Phishing-Angriffs oder die Anforderung einer Kennwortrücksetzung – können sich die Endbenutzer selbst helfen, anstatt direkt das Sicherheitsteam um Hilfe zu bitten.

Durch die Konsolidierung der am häufigsten benötigten Antworten, Informationen und Anfragen an einem Ort mit derselben Infrastruktur wie die IT-Abteilung wissen die Endbenutzer genau, wohin sie sich wenden müssen – schließlich rufen Sie genau dort alle IT-Informationen ab! – und versuchen nicht, das System zu umgehen.

****

Erwägen Sie, Folgendes in Ihr Sicherheits-Wiki aufzunehmen:

- **Alle aktuellen Richtlinien** – jeweils mit einer einsehbaren Liste, die zeigt, welche Benutzer und Geräte unter eine Richtlinie fallen, welche Einschränkungen oder Berechtigungen durch die Richtlinie gewährt werden, wie der Prozess der Ausnahmeanforderung und die Standorte aussehen und (vor allem) wie diese Richtlinie das Unternehmen schützt.
- **Wie man neue Passwörter oder Benutzernamen anfordert.**
- **Wie man einen neuen Anbieter oder eine neue Software zur Sicherheitsgenehmigung einreicht** – und warum das Sicherheitsteam eine einmalige Anwendung genehmigen muss und wie dies die Sicherheit des Unternehmens gewährleistet.
- **Wie 2FA** auf allen vom Unternehmen unterstützten Geräten und Anwendungen **implementiert werden kann**.
- **Roadmap zur Sicherheitsrichtlinie** für geplante künftige Implementierungen, die für die Kommunikation mit den internen Stakeholdern genehmigt wurden.



Automatisierung Nr. 2:

Vereinheitlichung der Warteschlagen von Sicherheitstickets mit kontextabhängigen Geräte- und Benutzerdaten

Dieselbe ITSM-Plattform mit Helpdesk-Tickets kann spezielle Warteschlangen für Sicherheitsfragen und Priorisierung bei Abhilfemaßnahmen bilden.

Sie könnten sogar Anforderungsformulare für den Dateizugriff oder für Ausnahmeregelungen innerhalb des Sicherheits-Wikis implementieren, um den Benutzern einen "Self-Service"-Support auf der Null-Ebene zu bieten.

Diese Formulare könnten dann die Anfragen der Benutzer in eine zentrale öffentliche Warteschlange einreihen, anstatt sie in den E-Mail-Postfächern zu verstreuen, wo sie von den Fachleuten wegen "höherer Prioritäten" ignoriert werden.

Dann können diese Anfragen leicht neu zugewiesen und von Mitarbeitenden der unteren Sicherheitsebene gelöst werden, so dass Ihr strategisches Personal für Aufgaben mit höherer Priorität zur Verfügung steht.

Außerdem kann Ihr Sicherheitsteam bei der Erstellung Ihres Sicherheits-Wikis auf die im Wiki verfassten Richtlinien verweisen, um seine Entscheidung über die Gewährung oder Verweigerung der angeforderten Berechtigungen zu untermauern – sogar für die Führungskräfte!

Automatisierung Nr. 3:

Wiederverwendung von abteilungsübergreifenden Tools für die proaktive Anwendung durch Sicherheitsteams

Dieselben Reparatur- und proaktiven IT-Automatisierungen, die auf der Grundlage bestimmter Einstellungen in ITAM und ITSM ausgelöst werden, können geklont und für eine Vielzahl von Sicherheitszwecken optimiert werden.

IT-Automatisierungen für Sicherheitsteams

Deprovisionierung

Stellen Sie sicher, dass die Anmeldeinformationen ausscheidender Mitarbeiter oder Lieferanten bei Vertragsbeendigung oder Eingabe des Benutzerstatus deaktiviert werden.

Baseline-Bewertungen

Automatisierungen können die Aktivitäten Ihres Unternehmens erfassen und zusammenfassen und Ihnen dabei helfen, zukünftige Sicherheitsauswirkungen auf die Produktivität und mögliche Eindringlinge zu erkennen.

Kennzeichnung bösartiger Aktivitäten

Warnung vor potenziellen internen Bedrohungen oder kompromittierten Konten, ausgelöst durch von der Norm abweichende CIs, die eine manuelle Geräte- oder Benutzerüberprüfung durch einen menschlichen Sicherheitsanalysten auslösen.

Überwachung der Markteinführung

Während des Rollouts von Patches oder Richtlinien können Automatisierungen so eingestellt werden, dass sie auf Unterbrechungen achten, und zwar auf der Grundlage vorher festgelegter Kadenzen und nach Prioritätenfür Benutzer- oder Geräteprofile, die von den aktuellen Workflows bestimmt werden.

UEM + Sicherheit

In diesem Abschnitt:

- Definition von UEM und MDM
- Sicherheitsspezifische Anwendungsfälle von UEM
- Shift-Left der Sicherheit mit UEM-Automatisierungen

Kurze Definitionen: UEM und MDM

Unified Enpoint Management (UEM)	Mobile Device Management (MDM)
UEMs sind eine IT-Technologieplattform, mit der Systemadministratoren mehrere Endpunkte – d. h. Geräte, Hardware und andere Technologien – über eine einzige Plattform oder ein einziges Dashboard verwalten können. UEMs decken ein breites Spektrum an Betriebssystemen und Gerätetypen von vielen verschiedenen Herstellern und Entwicklern ab.	MDM, das heute oft als "modernes" Gerätemanagement bezeichnet wird, waren einst eine eigenständige Nischentechnologie, die IT-Teams bei der Kontrolle und Durchsetzung von Richtlinien, Konfigurationen und Software auf Smartphones, Tablet-PCs und anderen Endpunkten, die MDMs-APIs unterstützen, half. Allerdings war MDM häufig auf Geräte mit bestimmten Betriebssystemen beschränkt, so dass IT-Teams mehrere MDMs gleichzeitig einsetzen mussten, um alle Geräte zu verwalten. Während Hersteller von Betriebssystemen und Nischengeräten immer noch Punkt-MDM-Produkte zur Verwaltung ihrer Endgeräte herausbringen, enthalten umfassende UEM-Lösungen MDM-Funktionen in ihren Plattformen.

UEM-Plattformen ermöglichen IT-Teams – und jetzt auch Sicherheitsteams! – ihre Hardware- und Software-Assets von einer einzigen Plattform und einem Dashboard aus zu verwalten, unabhängig von:

- Betriebssystem,
- Gerätetyp,
- Gerätestandort,
- eindeutigen Benutzerrechten.

Sicherheitsspezifische Anwendungsfälle von UEM

Die UEM- und MDM-Clients Ihres IT-Teams können für die Anforderungen des Sicherheitsteams neu konfiguriert werden, einschließlich:

Proaktive Gerätebereitstellung für neue Mitarbeiter unter Berücksichtigung sicherheitsrelevanter Zugriffskontrollen für bestimmte Geräte und Benutzerprofile

Robuste Internet of Things (IoT)-Kontrollen und Netzwerksegmentierungen, um schwer zu aktualisierende und schwer zu verfolgende Geräte zu sperren, die Hackern einen Zugang zu Kernnetzwerken bieten

Eine umfassende, betriebssystem- und geräteübergreifende Grundlage für zukünftige Erweiterungen und Anwendungsfälle – sowohl für die IT als auch für die Sicherheit! – wenn die Budgets steigen und sich der Bedarf erhöht

Sicherheit und Onboarding von Geräten

Ein einfacher Bereich, in dem die Sicherheit in die aktuellen IT-Prozesse einfließen kann, ist das Onboarding neuer Mitarbeitenden – vor allem, wenn Ihr Unternehmen derzeit hybride oder vollständige Remote-Bereitstellungen durchführt.

Schließlich ist die IT-Abteilung dafür verantwortlich, neue Geräte mit der entsprechenden Software und den entsprechenden Zugriffsberechtigungen für Endbenutzer bereitzustellen, die möglicherweise nie einen Fuß in das Büro setzen.

Dieser Prozess bietet einzigartige Möglichkeiten für die Sicherheit, um sicherzustellen, dass auch Remote-Benutzer und -Geräte von Anfang an sicher konfiguriert sind, bevor sie überhaupt eine Verbindung zum Unternehmensnetzwerk herstellen.

Mit UEM-Lösungen können IT-Administratoren außerdem vorkonfigurierte Benutzer- und Geräteprofile auf neuen Laptops oder PCs einrichten, die auf zuvor eingerichteten virtuellen Maschinen (VMs) basieren.

In Kombination mit einem ITSM können Personalverantwortliche ein Self-Service-Portal für Anforderungen und Berechtigungen nutzen, ohne dass jemand aus der IT-Abteilung vor der eigentlichen Anforderung und Geräte-/Profilkonfiguration aktiv beteiligt werden muss.

Wahrscheinlich hat Ihre IT-Abteilung bereits einen Prozess für das Onboarding neuer Benutzer eingerichtet. Fragen Sie sie nach Folgendem:

- Welche Verfahrensschritte sie bereits eingeführt haben
- Wie sie ihr UEM für die Bereitstellung nutzen und
- Wo Ihr Sicherheitspersonal und Ihre Sicherheitsrichtlinien in die Standardbetriebsverfahren einfließen könnten

Praktische Auswirkungen

Einbettung von Sicherheitsrichtlinien von Beginn an

In Interviews für eine von Forrester Consulting im Auftrag von Ivanti durchgeführte TEI-Studie schätzte ein Integrationsingenieur eines Schuhhändlers, dass sein Team früher zwei bis drei Tage pro Gerät für die Installation und Konfiguration von Software benötigte.

Nach der Implementierung von Ivanti Neurons für UEM stellte der Befragte jedoch fest:

"Sobald das Bild erstellt ist, installieren sie einfach Ivanti und ziehen das Gerät in alle Softwareaufgaben. Das ist in fünf bis zehn Minuten erledigt, und am Ende des Tages wird nur noch überprüft, ob Anträge vorliegen. Das spart definitiv Zeit im Onboarding-Prozess der Benutzer."

Die Konfigurationsanforderungen Ihres Teams sollten nicht erst im Nachhinein, "wenn Sie Zeit haben", sondern bereits beim Onboarding berücksichtigt werden.

Alles, was nötig ist, sind durchdachte Verhandlungen mit Ihren IT-Partnern über die am wenigsten störenden Standardberechtigungen, Anwendungen und Zugriffe, die jedes Benutzerprofil, Team oder jeder Gerätetyp in Ihrem Unternehmen benötigt."

FORRESTER®

Sicherheit und IoT

IoT-Endpunkt-Sicherheitsrichtlinien, die über UEM- und MDM-Clients bereitgestellt und durchgesetzt werden, bieten eine großartige Möglichkeit zur Wertschöpfung, wenn Ihr Sicherheitsteam versucht, den aktuellen IT-Stack wiederzuverwenden.

Schließlich machten IoT-Angriffe im Jahr 2021 mehr als 12 % aller weltweiten Malware-Angriffe aus – im Jahr 2019 waren es noch weniger als 1 % aller Malware-Angriffe.

Dennoch gaben 47 % der befragten IT-Experten an, dass ihr Unternehmen keine IoT-Compliance-Richtlinie hat.

Vielleicht liegt es weniger daran, dass diese Unternehmen keine IoT-Richtlinien haben, sondern eher daran, dass sie einfach nicht wissen, dass sie sie haben sollten oder wie sie diese umsetzen sollten.

Mit dem zusätzlichen Sicherheitsinput Ihrer Teams und Fachleute sind Sie jedoch in der Lage, anfällige internetfähige Geräte sowohl im Unternehmen als auch an entfernten Arbeitsplätzen durch die relativ einfache Netzwerksegmentierung und die aktiven Scan-Funktionen des UEMs zu beheben.

Praktische Auswirkungen

Bedrohungen für ein Aquariumthermometer

Ein nordamerikanisches Kasino entdeckte, welchen Schaden ein nicht verwaltetes IoT in seinem Betrieb anrichten kann, als Hacker eine Schwachstelle im Aquarium-Thermometer der Kasinolobby ausnutzten.

Da dieser internetfähige Tank im Netzwerk des Kasinos nicht ordnungsgemäß segmentiert war, drangen die Hacker seitlich in die Cloud-Infrastruktur des Kasinos ein und setzten ihren Angriff fort.

Sicherheit und OS-übergreifende Integrationen

In diesem eBook geht es zwar um die Wiederverwendung aktueller IT-Tools und -Plattformen, aber wir wissen, dass die Sicherheitsrisiken und -anforderungen Ihres Unternehmens irgendwann die Richtlinien und Durchsetzungsoptionen übersteigen, die Ihre aktuellen Tools bieten.

UEM-Lösungen bieten jedoch eine hervorragende Ausgangsposition für die Integration künftiger Sicherheitstool-Implementierungen in jedes Gerät und Benutzerzugangsprofil – unabhängig davon, wo sie sich befinden oder welches Betriebssystem sie verwenden.

Schließlich hat das UEM selbst einen Client, der direkt auf jedem eigenen und verwalteten Gerät des Unternehmens installiert ist.

Mit nur wenigen Klicks lassen sich andere Sicherheitstools über den UEM-Client in dasselbe Gerät einbinden, so dass die Endpunktsicherheit sofort verbessert wird, ohne die Produktivität der Endbenutzer in Ihrem Unternehmen zu beeinträchtigen – ein großer Gewinn für Ihre IT-Partner.

Zukünftige Sicherheitsintegrations-Optionen für die Bereitstellung über UEMs und MDMs

Patch-Management (PM) und risikobasiertes Schwachstellenmanagement (RBVM)

Das UEM selbst geht einen Schritt weiter als die von ITSM-, ITAM- und UEM-Plattformen ermöglichten Automatisierungen und Überwachungen. Es kann mit risikobasierten Patch- und Schwachstellenmanagementlösungen kombiniert werden, um eine nahtlose proaktive Risikoreaktion zur Behebung aktiv ausgenutzter Schwachstellen zu ermöglichen.

Durch die Verknüpfung von PM- und RBVM-Lösungen mit einer sicherheitskonfigurierten IT-Plattform können Sicherheits- und IT-Teams gleichermaßen die dringendsten Patches für aktiv ausgenutzte Schwachstellen kontextualisieren, die mit Ihrer aktuellen Asset-Umgebung und kritischen Workflow-Informationen aus der ITAM- / ITSM-Plattform abgeglichen und vom UEM gemäß den IT-Sicherheits-SLAs verteilt werden.

Mobile Bedrohungsabwehr (MTD)

Die Konfigurationen und Einstellungen eines UEM können sicher dazu beitragen, den anfänglichen Schaden zu begrenzen, der durch einen Klick auf einen Phishing-Link verursacht wird. Die gilt vor allem dann, wenn es mit einer Patching-Lösung gekoppelt ist, die die Möglichkeiten der Hacker, ihre Privilegien zu erweitern oder sich im Netzwerk zu bewegen, stark einschränkt! Sie ist weniger effektiv, als wenn die Richtlinie mit einer OS-übergreifenden Lösung zur Abwehr mobiler Bedrohungen (MTD) kombiniert wird.

Die besten MTD-Lösungen können über den UEM-Client eines angemeldeten Geräts – das entweder dem Unternehmen gehört oder in einem BYOD-Programm verwendet wird – ausgeführt werden, während sie potenziell bösartige Aktivitäten und Phishing-Angriffe dynamisch erkennen, segmentieren, unter Quarantäne stellen und Warnmeldungen ausgeben.

Das "Shift-Left" des Workloads der Sicherheitsabteilung mit UEM

Genauso wie ITAM und ITSM IT-fokussierte Automatisierungsmöglichkeiten für die Sicherheit boten, um den Shift-Left durchzuführen. und proaktiver mit zuvor manuellen Aufgaben umzugehen, bieten auch UEMs ihren Anteil an Automatisierungen, die sich als nützlich für Sicherheitsziele erweisen werden.

UEMs bieten einzigartige Automatisierungen und Implementierungen für Sicherheitsteams:

Garantie einer 100-prozentigen Einhaltung der Deaktivierungsrichtlinien für ausscheidende Mitarbeiter und "Zombie-Anmeldeinformationen" von Drittanbietern

Durchsetzen von Sicherheitsrichtlinien für aktiv verwaltete oder BYOD-Geräte, die auf Unternehmensnetzwerke zugreifen dürfen – unabhängig davon, ob sie sich im Büro befinden oder aus der Ferne arbeiten.

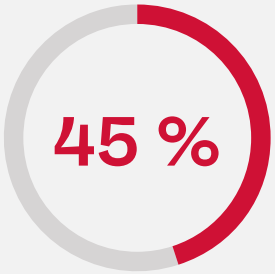
Durchsuchen kompilierter, sicherheitsrelevanter Geräteaufzeichnungen bei der Reaktion auf Vorfälle oder zur Kontextualisierung von Warnmeldungen.

1 Garantierte Einhaltung der Vorschriften zur Deaktivierung von "Zombie-Anmeldeinformationen"

In einer weltweiten Ivanti-Umfrage unter mehr als 900 Sicherheitsexperten gaben nur 68 % der Befragten an, dass ihr Unternehmen die Richtlinien zur Deprovisionierung von Anmeldeinformationen für gekündigte oder ausscheidende Mitarbeitende, Drittanbieter und andere Anbieter befolgt.

Tatsächlich gaben 45 % dieser Sicherheitsexperten an, dass sie den Verdacht haben, dass ehemalige Mitarbeitende und Auftragnehmende immer noch aktiven Zugang zu Unternehmenssystemen und -dateien haben, indem sie alte Anmeldeinformationen verwenden, die abgeschaltet wurden: "Zombie-Anmeldeinformationen"

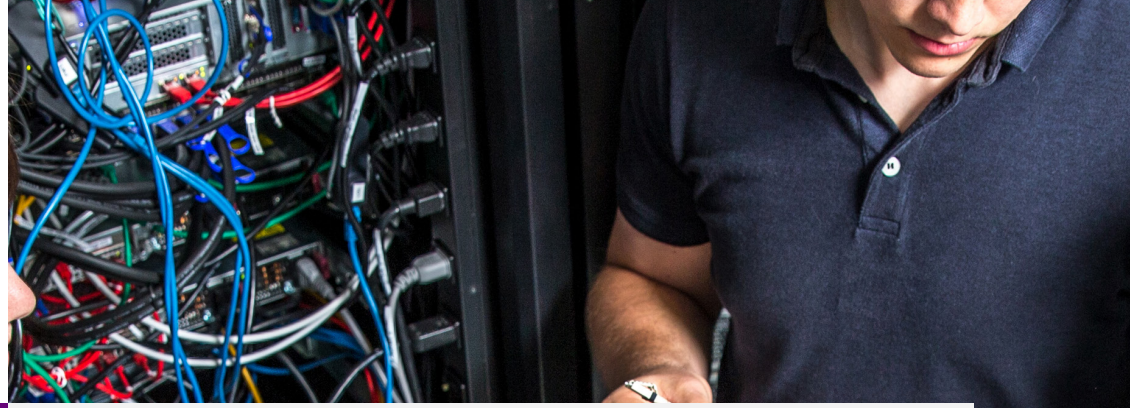
Automatisierungen innerhalb der UEM-Plattformen und der gerätegehosteten MDM-Clients ermöglichen die sofortige Deaktivierung von Zombie-Anmeldeinformationen, wenn das interne Profil eines Benutzers als "nicht mehr aktiv genutzt" markiert wird - so werden zukünftige externe Bedrohungen durch frühere Insider-Assets verhindert.



der Sicherheitsexperten geben an, dass sie entweder vermuten oder wissen, dass ehemalige Mitarbeiter und Auftragnehmer immer noch aktiven Zugang zu Systemen oder Dateien in Form von noch aktiven Benutzernamen, Kennwörtern und Anmeldeinformationen haben.

ivanti

2 Durchsetzung von Sicherheitsrichtlinien auf allen verwalteten Endgeräten - im Büro oder an Remote-Standorten.



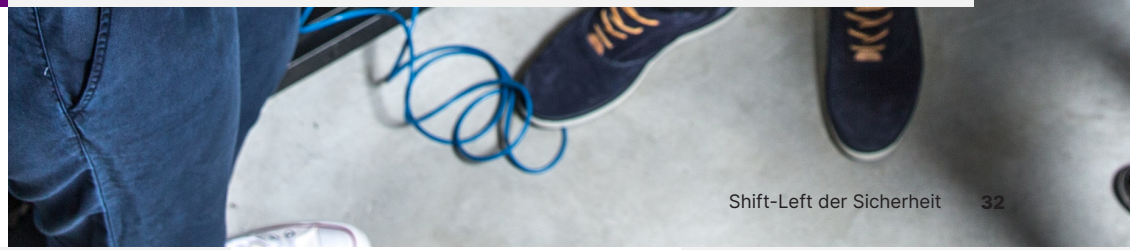
Auch wenn menschliches Versagen immer der schwächste Punkt jeder Sicherheitsstrategie bleiben wird, können Sicherheitslösungen und -richtlinien, die von der UEM-Plattform des IT-Teams durchgesetzt werden, dazu beitragen, einige der Risiken zu beseitigen, die von Ihren weniger aufmerksamen Endbenutzern ausgehen, insbesondere wenn diese an entfernten oder hybriden Arbeitsplätzen tätig sind.

So können beispielsweise viele anfängliche Erkundungs- und Eindringungstechniken, die von modernen Bedrohungsakteuren eingesetzt werden, durch eine ordnungsgemäße Bestandsaufnahme, Netzwerksegmentierung und Geräteüberwachung beseitigt werden.

Alle diese Sanierungsmaßnahmen können über UEM-Lösungen durchgeführt werden – mit den richtigen sicherheitsorientierten Konfigurationen und unterstützenden Funktionen.

Durch den Einsatz einer UEM-Lösung mit sicherheitsorientierten Richtlinien und Konfigurationen sind Unternehmen nicht mehr darauf angewiesen, dass sich Endbenutzer für benötigte Updates oder Sicherheitsanwendungen entscheiden.

Stattdessen melden sich UEM-verwaltete Geräte automatisch für den jeweiligen Aktualisierungsplan oder die Anwendungsinstallation an – ohne dass der Benutzer eingreifen muss!



3 Überprüfung von UEM-gehosteten Geräteaufzeichnungen während der Reaktion auf Vorfälle

Die von einer UEM-Plattform aufgezeichneten Geräte- und Benutzerprotokolle, die in der Regel von IT-Mitarbeitern verwaltet und überprüft werden, um die Geräte der Endbenutzer besser reparieren zu können, können auch für Sicherheitszwecke verwendet werden.

Wenn das Unternehmen Grund zu der Annahme hat, dass bestimmte Mitarbeitende eine Insider-Bedrohung darstellen könnten, kann das Sicherheitsteam beispielsweise die Aufzeichnungen eines Geräts auf Anzeichen überprüfen, dass Tools auf Systemadministrator-Ebene wie PowerShell illegal auf dem Gerät eines Benutzers installiert und verwendet wurden.

Oder das System eines Unternehmens löst einen Alarm aus, wenn ein Standardbenutzer plötzlich administrative Netzwerkbefehle auf dem vom Unternehmen verwalteten Gerät ausführt.

Solche Aktivitäten können ein Zeichen dafür sein, dass es sich gar nicht um den autorisierten Benutzer handelt, sondern um einen Hacker, der sich hinter den authentischen (aber kompromittierten) Anmeldeinformationen dieses Benutzers versteckt und versucht, seine Rechte im Unternehmensnetzwerk zu erweitern.

Mit den richtigen Konfigurationen, Warnmeldungen und Sicherheitstools können diese Aktivitäten auf einem Endgerät oder einem mobilen Gerät erkannt werden, lange bevor der Hacker sich im Netzwerk des Unternehmens bewegt oder erhöhte Administratorrechte erhält.

Und da steigende Cyberversicherungstarife die ohnehin schon angespannte finanzielle Situation von Unternehmen weiter belasten, werden sowohl IT- als auch Sicherheitsteams feststellen, dass es aus finanzieller Sicht sinnvoll ist, strengere Richtlinien und Benutzeraktivitätswarnungen durchzusetzen, um proaktiv Risiken zu beseitigen und Versicherungsprämien zu senken.

04

Alle Wege führen zu DEX

In diesem Abschnitt:

1. Warum sich sowohl Sicherheits- als auch IT-Teams für DEX interessieren (sollten)
2. Wie Backend DEX von gemeinsamen Tech-Stacks technischen Administratoren hilft

DEX: der verborgene Vorteil der Sicherheit beim Shift-Left der IT

In diesem Leitfaden haben wir gezeigt, dass sich Sicherheitsteams vom Einsatz reaktiver Notfalltaktiken zu proaktiveren und reaktionsfähigeren Cyber-Ökosystemen entwickeln und gleichzeitig ihren technologischen Fußabdruck verkleinern können – indem sie einfach die bereits von ihrem IT-Team unterstützten ITSM-, ITAM- und UEM-Funktionalitäten nutzen.

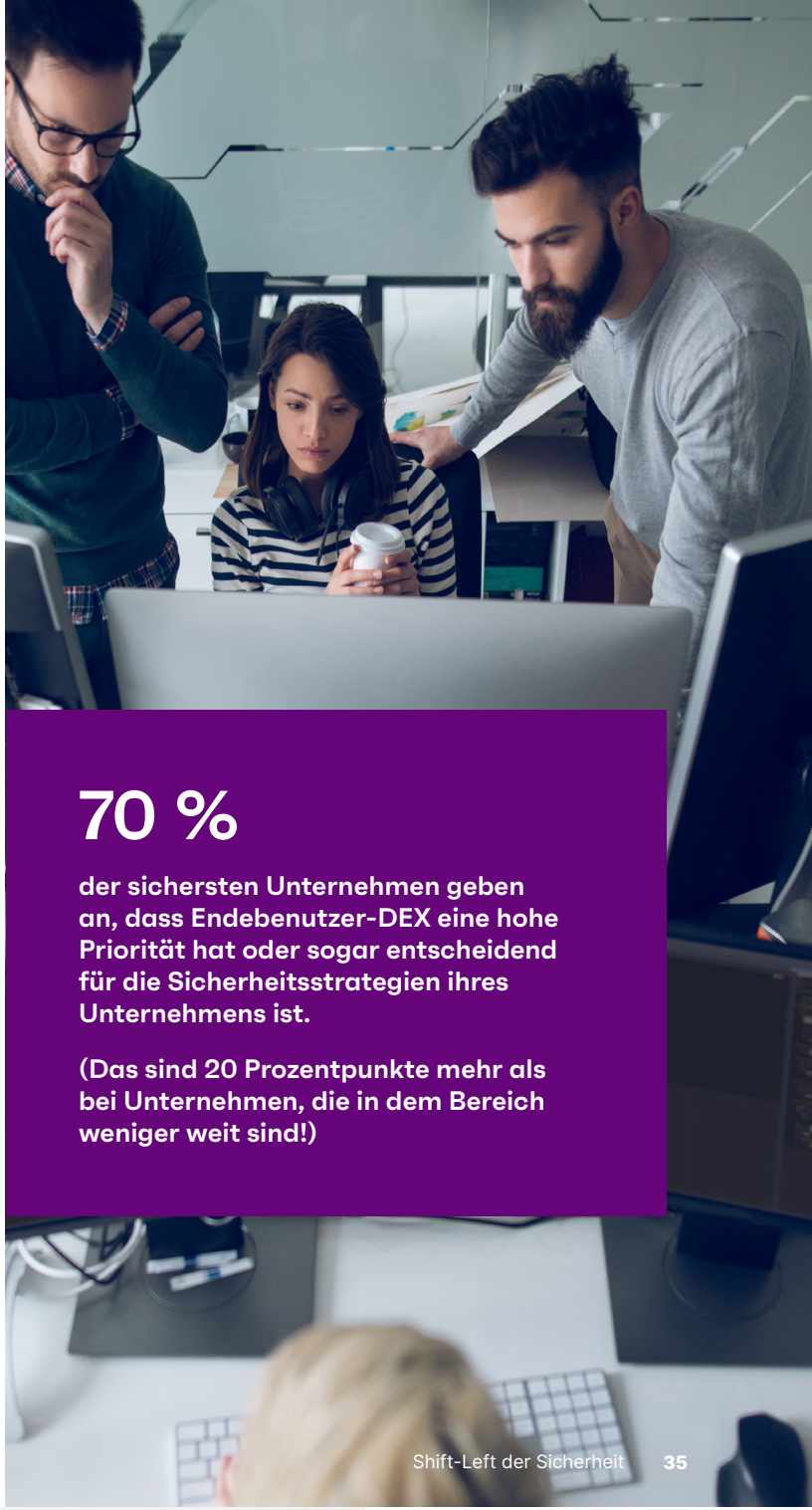
Es gibt jedoch noch einen weiteren Vorteil, den Unternehmen aus der Kombination und Konsolidierung ihrer IT- und Sicherheitstools ziehen können: eine verbesserte digitale Mitarbeitererfahrung (DEX).

Diese DEX-Vorteile können sich auf das gesamte Unternehmen erstrecken, und zwar nicht nur auf die Endbenutzer, sondern auch auf Anwendungsfälle, die sich auf Folgendes konzentrieren:

Sicherheitsbedarf

IT-Bedarf

Allgemeiner technischer Verwaltungsbedarf



70 %

der sichersten Unternehmen geben an, dass Endebenutzer-DEX eine hohe Priorität hat oder sogar entscheidend für die Sicherheitsstrategien ihres Unternehmens ist.

(Das sind 20 Prozentpunkte mehr als bei Unternehmen, die in dem Bereich weniger weit sind!)

Endbenutzer-DEX kommt sowohl der Sicherheit als auch der IT zugute

Während die digitale Mitarbeitererfahrung für Sicherheits- und IT-Abteilungen aus unterschiedlichen Gründen gleichermaßen interessant ist, ist die Verbesserung des Endbenutzer-DEX ein Gewinn für alle Beteiligten!

DEX-Vorteile für die Sicherheit

DEX-Vorteil	Warum sie für Sicherheitsteams interessant ist
Bessere Benutzererfahrungen schützen vor Schatten-IT.	Mitarbeitende nutzen nicht genehmigte Geräte oder Anwendungen – Schatten-IT –, wenn sie die Unternehmensversion als umständlich oder frustrierend empfinden. Diese Schatten-IT kann Schwachstellen in ein Netzwerk einbringen und Unternehmen der Cyberkriminalität aussetzen: 12,8 % der Cloud-basierten Cyberangriffe im Jahr 2022 betrafen Schatten-IT. Durch die Priorisierung des Endbenutzer-DEX können Unternehmen die Arbeit mit sicherheitsrelevanten Anwendungen und Geräten für Endbenutzer vereinfachen und gleichzeitig die Schatten-IT reduzieren. Warum sollten sie sich die Mühe machen, eine Drittanbieter-Anwendung zu installieren, ihre vorhandene Anwendung funktioniert?
Backend, "ausgeblendete" Implementierungen von Sicherheitsrichtlinien, die die stillschweigende Einhaltung durch die Benutzer unterstützen.	Unternehmen können (und tun dies auch!) offenkundige Richtlinien ausgeben, die ihre Endbenutzer dazu verpflichten, bestimmte Aktionen zu unternehmen oder zu vermeiden, um ihre Sicherheit zu gewährleisten. Oder... Sicherheitsteams könnten einfach Backend-Automatisierungen implementieren, die Richtlinien für jedes verwaltete Gerät und jedes Netzwerkbenutzerprofil unbemerkt im Hintergrund durchsetzen. Die Benutzer erfahren nur dann von diesen Richtlinien, wenn sie eine unbefugte Aktion durchführen – andernfalls werden sie nie erfahren, dass diese Einschränkungen existieren. Diese DEX-freundlichen Sicherheitsimplementierungen bedeuten, dass Unternehmen nicht mehr auf den guten Willen und das Gedächtnis des durchschnittlichen Endbenutzers angewiesen sind, sondern auf solide Backend-Implementierungen, bei denen der Benutzer nichts tun muss!
Hybrid-kompatible Sicherheitskontrollen bieten standortunabhängigen Benutzerkomfort.	Angesichts der zunehmenden Anzahl an Remote- und Hybrid-Arbeitskräften können sich Sicherheitsteams nicht mehr auf den grundlegenden "Walled Garden"-Ansatz für die Netzwerk- oder Endpunktsicherheit verlassen... oder darauf, dass Benutzer in der Lage und bereit sind, potenziell kompromittierte Rechner mit ins Büro zu bringen. Der Einsatz von Backend-IT-Plattformen wie UEMs und ITAMs, die jeden Gerätetyp mit jedem Betriebssystem tracken, verwalten und sichern können – sowohl vor Ort als auch aus der Ferne! – sorgt dafür, dass Sicherheitsteams die Sicherheit von Unternehmen gewährleisten können, ohne dass die Benutzer ins Büro kommen müssen.

Schon gewusst?

Die IT-Abteilung Ihres Unternehmens hat möglicherweise bereits DEX-Initiativen zur Verbesserung der Endbenutzerproduktivität durchgeführt.

Durch die Zusammenarbeit mit dem Sicherheitsteam haben Ihre IT-Führungskräfte ein zusätzliches Druckmittel, um den nun gemeinsam genutzten Technologie-Stack zu rechtfertigen. Dadurch kann das DEX-Programm weiter verfolgt werden, zeigt seinen Nutzen für das Unternehmen konkreter und begründet so weitere Investitionen.

DEX-Vorteile für die IT

DEX-Vorteil	Warum sie für IT-Teams interessant ist
Weniger Benutzerprobleme bedeuten weniger Service-Desk-Tickets und schnellere Servicebereitstellung.	Wenn die Geräte so funktionieren, wie es die Benutzer wünschen – ohne Unterbrechungen durch Neustarts oder langsame Verarbeitung aufgrund von geringem Arbeitsspeicher – dann haben sie keinen Grund, Helpdesk-Tickets einzureichen. Als eine Religionsgemeinschaft ein auf DEX basierendes ITSM implementierte, konnte ihr IT-Team die Anzahl der Tickets reduzieren und die Service-Erfahrung der Helpdesk-Mitarbeitenden um 90 % verbessern.
Das selbständige Beheben von Fehlern durch die Benutzer senkt die IT-Arbeitskosten.	Wenn Formulare für Fehlerbehebung und Anfragen dort abgelegt werden, wo Endbenutzer sie finden und verwenden können, dann können die Benutzer – und nicht Ihre hoch bezahlten IT-Mitarbeitenden – ihre Probleme selbst lösen. Nach der Implementierung eines ITSM-basierten Self-Service-Portals mit ergänzender Backend-Technologie stellte eine Universität fest, dass ihre neue IT-Technologie sowohl von den Studierenden als auch von den Mitarbeitenden uneingeschränkt akzeptiert wurde – mit einer breiten Akzeptanz der neuen Selbsthilfefunktionalität auf netzgebundenen Geräten.
DEX-Technologien lösen die grundlegenden Probleme und beschränken sich nicht auf oberflächliche Korrekturen.	Durch DEX-fokussierte Tech-Stacks können IT-Teams Geräte und ihre Benutzeraktivitäten schnell einsehen und bewerten, unabhängig davon, wo auf der Welt sich das fehlerhafte Gerät befindet. Diese Erkenntnisse – in Verbindung mit ausgefeilten Automatisierungen, die auch banalere und alltägliche Probleme "beheben" können – ermöglichen es den IT-Experten, Probleme schneller zu diagnostizieren und zu lösen. Das Gerät wird beim ersten Mal, beim ersten Ticket, repariert – der Endnutzer muss IT nicht wegen desselben Problems immer wieder kontaktieren.

Administrator-DEX profitiert von gemeinsamen Tech-Stacks

Hervorragende digitale Mitarbeitererfahrungen machen nicht bei den Endbenutzern halt. Die Administratoren, die diese Technologie nutzen, sollten auch von einer guten DEX profitieren!

Zusätzliche DEX-Vorteile für Sicherheits- und IT-Administratoren

DEX-Vorteil	Warum sie für Admins interessant ist
Arbeitstools und -geräte helfen den Benutzern, die Aufgaben zu erfüllen, für die sie bezahlt werden!	31 % der befragten Sicherheits- und IT-Fachleute spielen mit dem Gedanken, ihre derzeitige Stelle zu kündigen – zum Teil aufgrund von technologischen Schwierigkeiten. Warum sollten Sie Ihr wertvollstes Personal vergraulen, wenn die Verbesserung ihrer Erfahrungen mit Ihrer Technologie dazu beitragen kann, sie auf einem umkämpften Arbeitsmarkt zu halten?
Gemeinsame Plattformen und Dashboards mit einem DEX-Fokus bedeuten mehr Kompetenz und ein gemeinsames Verständnis über Abteilungsgrenzen hinweg.	Intuitive, abteilungsübergreifende Tools ermöglichen ein gemeinsames Verständnis von Informationen und eine nahtlose Darstellung von Problemen. Dieses gemeinsame Wissen und der gemeinsame Kontext erhöhen die Sensibilität, verringern Missverständnisse und verbessern die Zusammenarbeit in allen Abteilungen. Außerdem lassen sich die Kenntnisse schnell von einer Abteilung auf die andere übertragen, da alle ein grundlegendes Verständnis der zugrunde liegenden Plattformen haben.
Durch gemeinsam genutzte Tech-Stacks könnten jährlich bis zu 9 % der verlorenen Verwaltungsproduktivität ausgeglichen werden.	Einem kürzlich erschienenen Artikel der Harvard Business Review zufolge verlieren technische Mitarbeitende, die häufig zwischen verschiedenen Programmen hin- und herwechseln, viel produktive Zeit. Computerorientierte Wissensarbeiter wechseln im Durchschnitt 1.200 Mal pro Tag zwischen Plattformen, Schnittstellen, Bildschirmen und anderen Mikroaufgaben hin und her – und verschwenden damit schätzungsweise vier Stunden pro Arbeitswoche und 9 % ihrer bezahlten Jahresarbeitszeit. Eine konsolidierte, gemeinsame Plattform – oder zumindest ein Tech-Stack mit ähnlichen Benutzeroberflächen und Dashboards! – verringert die Belastung der Sicherheits- und IT-Administratoren durch das Hin- und Herwechseln und verbessert die Konzentration auf die zugewiesenen Aufgaben.

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/fa2e133f20a8
- 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

- 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://www.ivanti.com/resources/v/doc/ivi/2700/4e528f833de3
- 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
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://www.sans.org/white-papers/sans-2022-cloud-security-survey
- 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

Shift-Left der Sicherheit

Wie man reaktionsfähige Sicherheitsumgebungen mit aktuellen IT-Tools betreibt

ivanti

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