ivanti

Transparenz erhöhen, klar sehen, entschlossen handeln

Bessere IT-Einblicke für
bessere Geschäftsergebnisse

Inhaltsverzeichnis

Einführung

Wenn Sie nichts anderes aus diesem Whitepaper mitnehmen, überdenken Sie dies:

Ein vollständiger Überblick über die Assets, Services, Sicherheitsaufstellung, Prozesse und Ergebnisse Ihrer IT-Abteilung bildet die Grundlage für die ordnungsgemäße Verwaltung, Sicherung und Optimierung Ihres IT-Bestands. Sie werden klarer sehen, entschlossener handeln und effizienter werden. Dies wiederum wird Ihnen helfen, Kosten und zukünftige Budgets zu optimieren, die Erfahrung Ihrer Kunden und Mitarbeiter zu verbessern und Ihr Team produktiver und effizienter zu positionieren.

Und wer würde das heutzutage angesichts stark regulierter Industrien und Compliance-Vorschriften nicht wollen; die Notwendigkeit der Vorgabe einer klaren Richtung für Patching, Kostenoptimierung, Anwendungskontrolle und den Verbleib von Assets und das Ziel der IT-Abteilung, nicht mehr nur eine Kostenstelle zu sein, sondern „mit am Verhandlungstisch zu sitzen“ und ein Zentrum der Innovation zu werden.

Tatsache ist, dass volle Transparenz nach und nach erreich wird – mit ersten Schritten, gefolgt von weiteren Schritten. Ein Beispiel:

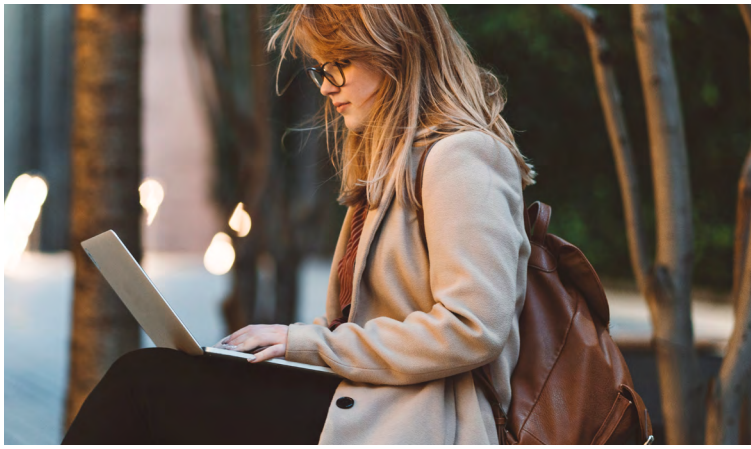
- Wie können Sie ohne eine Baseline als Ausgangspunkt einschätzen, was Ihr Status quo im Hinblick auf Assets, Sicherheit, Prozesse und Reifegrad ist, oder wie viel und welche Arbeit auf das IT-Team zukommt?
- Wie können Sie etwas in Ihrer Umgebung verwalten, von dem Sie nichts wissen?
- Wie können Sie mit dem gleichen Budget und den gleichen IT-Ressourcen mehr Wert für das Unternehmen schaffen?
- Wie können Sie mit unausgereiften und/oder manuellen Methoden, die die Transparenz auf breiter Front beschränken, eine umfassendere Unterstützung für ein breiteres Spektrum von Endpunkt-Gerätetypen bieten?

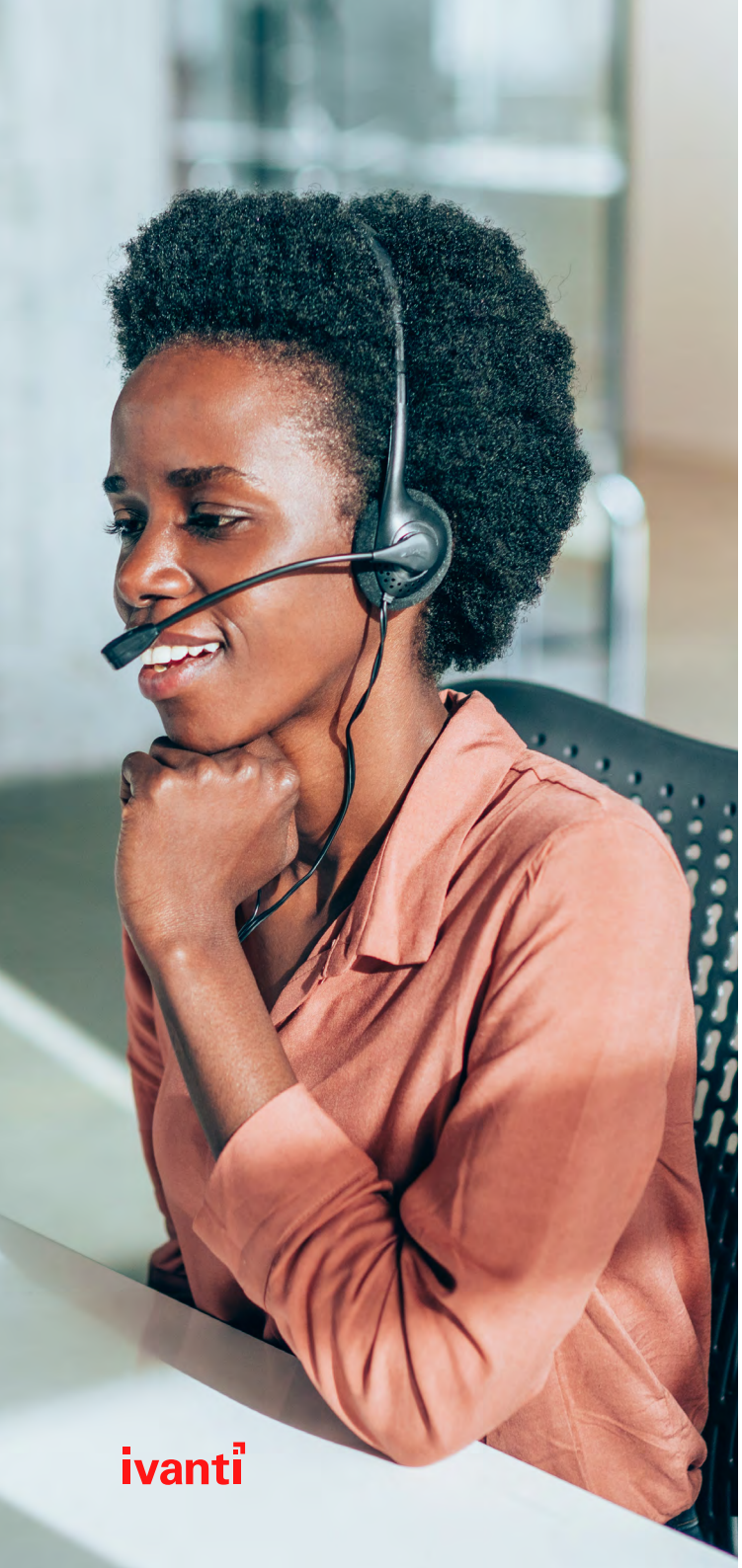
Ivanti bringt Licht in jeden Winkel Ihrer Unternehmens-IT-Landschaft

Transparenz muss zur grundlegenden Praxis werden, und bewährte Lösungen von Ivanti rücken jeden Aspekt der IT-Infrastruktur Ihres Unternehmens in den Mittelpunkt. Ein vereinheitlichter IT-Ansatz bringt die IT-Teams aus den Bereichen IT-Servicemanagement, IT-Assetmanagement, Endpoint-Security-Management, Nutzer- und Workspace-Management zusammen – organisiert unter den Eckpfeilern Enterprise Service Management und Unified Endpoint Management. Dank größerer Klarheit und Sichtbarkeit sind Sie mit Ihren Nutzern, Services und Anlagen im gesamten Unternehmen besser synchronisiert – und mit Ihrer IT-Landschaft, Ihrer Sicherheitsaufstellung sowie Ihren Prozessen und Daten. Sie haben die Mittel, um mehr von Ihren strategischen Zielen zu erreichen. strategic objectives.

Über dieses Whitepaper

Dieses Whitepaper bietet sechs kurze, anschauliche Anwendungsfälle und Forschungsdatenpunkte, die Ihnen helfen zu beurteilen, wo Ihre IT-Abteilung mehr Klarheit und Transparenz erreichen könnte und lädt Sie ein, Ivanti Lösungen zu evaluieren, die nachweislich dazu beitragen, Unternehmen dabei zu unterstützen.





Mangelnde Sichtbarkeit: Sechs Anwendungsfälle

Betrachten Sie die folgenden sechs Anwendungsszenarien und Schwachpunkte, die typischerweise mit einem Mangel an Transparenz verbunden sind:

1 Laptops in Zeitlupe

Ein Helpdesk-Mitarbeiter bemerkt einen Anstieg bei Anrufen, die Probleme mit schwacher Leistung von Laptops betreffen. Nach zeitaufwendigem Nachfassen erfährt der Helpdesk-Mitarbeiter, dass ein leitender Angestellter eine Woche zuvor von einer Konferenz mit einer Anwendung zurückkam, die er für eine „Killer-App“ hielt und anregte, diese von seinem USB-Laufwerk herunterzuladen, was zur Wiederverwendung derselben Lizenz führte. Die weitere Untersuchung ergab ferner, dass die App ein Ressourcenfresser ist. Unklar ist jedoch, auf wie vielen Laptops die Anwendung jetzt installiert ist.

Viele IT-Abteilungen haben heute noch unausgereifte und/oder manuelle Verfahren, die die Transparenz auf breiter Front einschränken. Ohne Transparenz ist es sehr schwierig, Hardware und Software zu erkennen, zu verwalten und zu schützen sowie die Softwarenutzung effektiv zu verwalten.

Das obige Szenario spricht mehrere Unbekannte an:

- Das Risiko der Non-Compliance aufgrund der Verwendung von nicht lizenzierter Software
- Schatten-IT, d. h. Beschäftigte, die die IT-Abteilung umgehen und nicht autorisierte Software installieren
- Die Anzahl der potenziell betroffenen Laptops
- Die Gesamtzahl der in diesem Zusammenhang eingehenden Incidents
- Durch nicht autorisierte Installation und Nutzung von Software erzeugte Sicherheitsrisiken
- Unbekannte Lizenz-True-up-Risiken

Um die Botschaft zu untermauern, dass man nicht verwalten, schützen und optimieren kann, vom dessen Existenz man nichts weiß und das auch nicht einfach zu sehen ist, heißt es in einem Whitepaper von Ernst & Young (EY) mit dem Titel „Data Validation the Best

43 %

der befragten Unternehmen verwenden immer noch Kalkulationstabellen.

50 %

verwenden eine Endpunkt-Managementlösung.

45 %

nutzen Inventarisierungstools als eine ihrer Ressourcen.

Practice for Data Quality in Fixed Asset Management“ (Datenvalidierung – die beste Praxis für Datenqualität in der Verwaltung von Anlagevermögen), dass 56 % der Unternehmen den Standort ihrer Anlagegüter einmal im Jahr überprüfen, während 10 % bis 15 % ihre Anlagen seit mehr als fünf Jahren nicht mehr überprüft haben.

Mangels formellem IT-Assetmanagement-Programm (ITAM) verlassen sich Teams oft ausschließlich auf Active Directory oder grundlegende Bestandsinformationen aus Endpunkt-Managementlösungen. Bezüglich der Nachverfolgung von Assets ergab die von Ivanti im Dezember 2019 in Auftrag gegebene ITXM-Forschungsstudie Folgendes. Bitte beachten Sie, dass Unternehmen möglicherweise mehrere dieser Optionen nutzen:

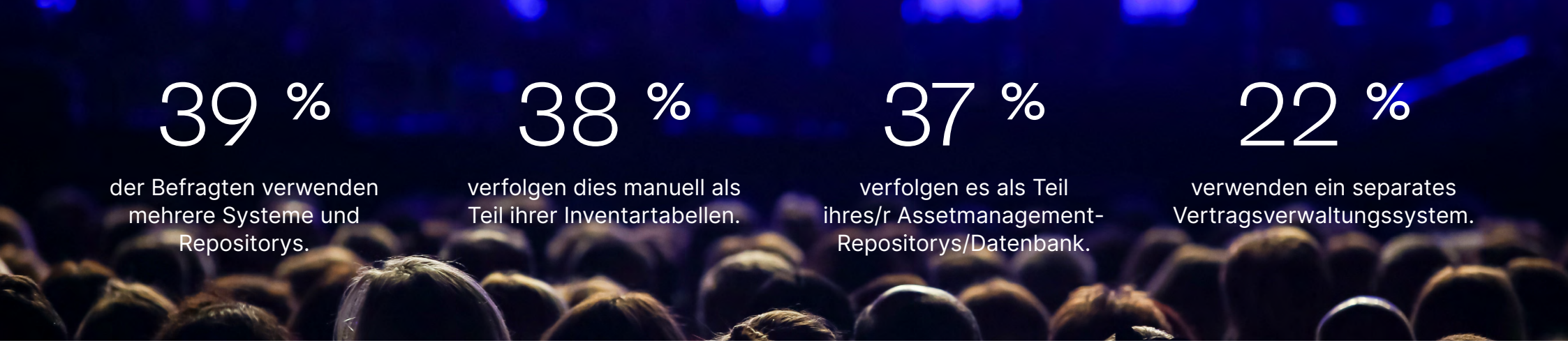
Mehrere Datenquellen, die miteinander kombiniert werden müssen, wie ITSM-, ITAM- und SAM-Daten, schränken die Geschwindigkeit ein, mit der die benötigten Einblicke und Transparenz insgesamt gewonnen werden können. Nach Untersuchungen von Enterprise Management Associates (EMA) verfügen 50 % der Unternehmen über 12 oder mehr Erkennungs- und/oder Inventarisierungstools, und 11 % besitzen mehr als 30 Tools. Im Durchschnitt verbringen Unternehmen 10 Stunden pro Woche mit der Lösung von Datengenauigkeitsproblemen, während 32 % mehr als 25 Stunden pro Woche damit verbringen.

Kurz gesagt, mangelnde Transparenz bedeutet, dass Sie nicht verwalten, schützen und optimieren können, von dem Sie nicht wissen, dass Sie es haben und das Sie nicht ohne Weiteres sehen können. Ivanti Lösungen nutzen leistungsstarke Datenimport-Funktionen, mit denen Sie Daten aus verschiedenen Quellen wie Tabellenkalkulationen, Inventarisierungstools, Barcode-Scans, Suchdiensten usw. kombinieren können, um die tatsächlichen Daten mit den gefundenen Daten zu vergleichen und Diskrepanzen zu melden. Mit diesen Erkenntnissen können Entscheidungsträger Annahmen validieren und sicherstellen, dass die Assetinformationen stets aktuell und genau sind.

2 Router im Wareneingang

Das Netzwerk-Ops-Team erhält einen Anruf vom Wareneingang. Gerade ist eine Palette mit neuen Routern eingetroffen. Das Ops-Team beginnt mit der Konfiguration der neuen Router, um einige ältere Router zu ersetzen, bevor es merkt, dass niemand die neuen Router bestellt hat.

Mangelnde Transparenz führt zu vielen Unbekannten. Wie sieht die Beschaffungsgeschichte aus? Welches sind die bevorzugten Anbieter und Auftragserfüllungswege? Welche Sicherheitsrisiken



gehen möglicherweise von nicht autorisierter Hardware aus, die mit dem Netzwerk verbunden wird?

Die von Ivanti in Auftrag gegebene ITXM-Studie (vom Dezember 2019), die bereits erwähnt wurde, fragte danach, wie Unternehmen Kaufdaten, Verträge und Garantiedaten für ihre IT-Assets verfolgen und überwachen. Die Studie ergab Folgendes. Bitte beachten Sie auch hier, dass Unternehmen möglicherweise mehrere dieser Optionen nutzen:

Der Einblick in Daten und Datenquellen, d. h. zu wissen, welche Daten es gibt und alles an einem Ort zu haben, wird viel dazu beitragen, die oben genannten Schwachstellen zu entschärfen. Dies sollte zu Daten führen, die konsistent, genau und vertrauenswürdig sind.

Wie in der Einleitung erwähnt, gilt bei einer engen Abstimmung, Integration und Automatisierung von Enterprise Service Management und Unified Endpoint Management Folgendes:

- Sie können die Erkenntnisse aus der Asseterkennung nutzen, um Vorhersagen zu treffen und präskriptive Maßnahmen für problematische Assettypen, Modelle und Anbieterinformationen zu ergreifen.
- Sie profitieren von tieferen Einblicken, um das Lieferantenmanagement, die Compliance und die Optimierung der Gewährleistung zu verbessern.
- IT-Mitarbeiter werden von reaktiven oder unnötigen Aktivitäten befreit und können sich auf strategischere Projekte konzentrieren.
- Sicherheitsrisiken werden reduziert, wenn man weiß, welche Hardware zur Nutzung zugelassen ist.
- Sie können mehr erreichen, während Sie die Kosten und den Verwaltungsaufwand minimieren und dem Unternehmen direkt mehr Wert bieten.

3 Pfennigfuchserei

Der CIO weist die Mitarbeiter an, sich um Budgeteinsparungen für das laufende Jahr zu bemühen. Der VP of Operations möchte sehen, ob sie den Laptop-Aktualisierungszyklus verlängern können, doch es ist ungewiss, wie viele Laptops betroffen wären, welche Mitarbeiter davon betroffen sein könnten, welche potenziellen Probleme entstehen würden und wie viel Budget dadurch tatsächlich eingespart werden könnte.

Zu den Problemen, die bei diesem Anwendungsfall zu Tage treten, gehören ein unbekannter Incident vom Typ Laptop und eine unbekannte Lieferantenhistorie, eine fehlende konsistente Verfolgung des gesamten Assetlebenszyklus, um den Zustand und die Leistung von Laptoptypen zu bestimmen, und eine unbekannte Patching-Historie. Es ist auch nicht bekannt, welche Mitarbeiter davon betroffen sein könnten.

Mit den richtigen Einblicken konnte ein Ivanti Kunde die Hardware-Aktualisierungszyklen um sechs bis zwölf Monate verlängern, wodurch die IT-Organisation anfänglich 1,5 Millionen US-Dollar einsparen konnte, ohne dass sich die Vorfallsraten erhöhten oder die Servicequalität für die Endnutzer beeinträchtigt wurde

Das ergab auch die Forschungsstudie zu ITXM vom Dezember 2019:

Das Verständnis der Lebenszyklen von Assets, deren Leistung, der Einhaltung von Vorschriften und der Auswirkungen auf die Kosten ist besonders wichtig für Unternehmen, die in stark regulierten Branchen tätig sind. Die Medizingeräteindustrie und die staatliche Regulierung mobiler Geräte (MDR) und die damit verbundenen Vorschriften der Europäischen Datenbank für Medizinprodukte (EUDAMED) in der Europäischen Union sind Beispiele dafür.

28 %

der befragten IT-Fachleute verbrachten jede Woche Stunden für den Support von Assets, deren Garantie bzw. Supportverträge abgelaufen waren.

20 %

von ihnen gaben an, dass sie keine Einblicke darin hätten, welche Assets veraltet sind.

4 Schneckenpost

Eine Flut von Anrufen empfängt die Helpdesk-Mitarbeiter gleich am Morgen. E-Mail „funktioniert nicht“ oder ist „extrem langsam“. Nach mehreren Anrufen bei anderen IT-Teams kommt das IT-Operations-Team zu dem Schluss, dass jemand die E-Mail-Anwendung über Nacht aktualisiert hatte und der aktuelle Server die daraus resultierenden Konfigurationsänderungen nicht verarbeiten konnte, was zu Leistungsproblemen führte. Es ist nicht sofort klar, ob die erforderliche Hardware vorhanden ist, um die Probleme zu beheben.

Zu den in diesem Fall aus der mangelnden Transparenz resultierenden Probleme gehören eine unklare Änderungs- und Konfigurationshistorie, kein Einblick in zukünftige Änderungen, keine Analyse der Auswirkungen von Änderungen und Risiken sowie ein unbekannter Hardwarebestand.

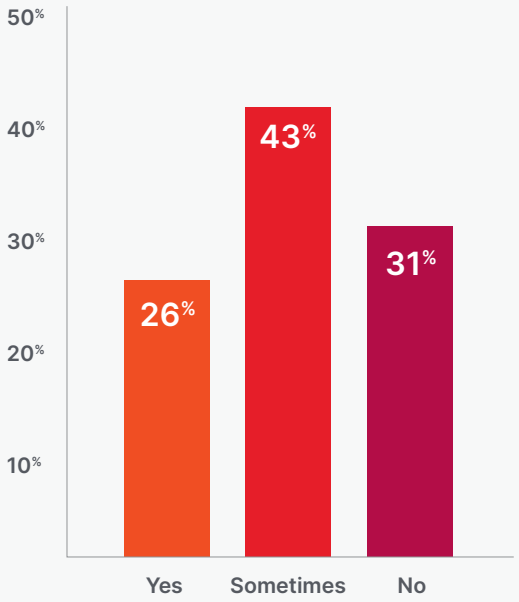
Unternehmen entwickeln IT-Ziele, um ihren Reifegrad zu erhöhen und setzen Automatisierung ein, um Effizienzgewinne zu erzielen. Doch viele vergessen den entscheidenden ersten Schritt: die Definition einer Baseline als Ausgangsbasis. Dies bedeutet: 1) einen vollständigen Einblick in die Prozesse und Maßnahmen zu erhalten, die sich auf die wichtigsten Services und die zugrunde liegenden Assets auswirken, z. B. auf das Change-Management; und 2) ein vollständiges Verständnis der Muster bei Incidents, der Ursachen von Ausfällen und mehr zu erlangen, um eine Ausgangsbasis zu schaffen, von der aus Verbesserungen möglich sind.

Tatsache ist, dass schlechte Systeme und fehlende Ressourcen trotz bester Bemühungen der IT-Teams taktische und reaktive Service- und Supportaktivitäten nach sich ziehen können. Ein systematischer Ansatz, der mehr als nur kurzfristige Ergebnisse bringt, ist nur bedingt möglich, und Probleme werden ad hoc gelöst. Hinzu kommt Folgendes:

- Viele Prozesse sind manuell, es mangelt an konsistenten IT-Abläufen oder Standards.
- Die Transparenz des Status oder der Auswirkungen ist geringer als gewünscht, mit minimalen bis gar keinen Berichtsmöglichkeiten.
- Die laufenden Kosten und Risiken sind hoch, die Lösungsfristen oft länger und die Servicequalität ist niedrig.
- Das leitende Management ist sich möglicherweise nicht über die Bedeutung des Serviceteams im Klaren und unterstützt größere Investitionen nur selten.

Survey:
The Impact of Aligning It Service & Asset Management Processes

Do your service management processes and request workflows automatically have visibility into asset information and relationships?



Bedeutung des Serviceteams im Klaren und unterstützt größere Investitionen nur selten.

Es lohnt sich auch, die untenstehende Erkenntnis aus der ITXM-Studie vom Dezember 2019 hervorzuheben, die aufzeigt, ob die Servicemanagementprozesse und Request-Workflows von Unternehmen automatisch Einblick in Assetinformationen und -beziehungen geben:

Wie Sie sehen können, gaben weniger als ein Drittel der Befragten an, dass sie Einblick in Assetinformationen haben, während die restlichen zwei Drittel nur manchmal oder gar keinen Einblick in Assetinformationen haben.

Laut derselben Studie erwarten IT-Fachleute mit Hilfe von integrierten IT-Servicemanagement- und IT-Assetmanagement-Prozessen und -Daten die folgenden Verbesserungen:

- Höhere Transparenz des IT-Bestands – 63 %
- Höhere Produktivität des IT-Personals – 59 %
- Kostenoptimierung – 54 %
- Verbesserte Servicebereitstellung – 53 %

5 Laptop-Sperre

Ein Vertriebsmitarbeiter ruft beim Helpdesk an und meldet, dass er aus seinem Laptop ausgesperrt ist. Auf dem Bildschirm sei die Meldung erschienen, eine andere Nummer anzurufen, um die Sperre aufzuheben. Er erwähnt auch, dass er auf einen Link in einer E-Mail geklickt habe, von der er dachte, sie käme von einem Partner, mit dem er schon einmal zusammengearbeitet habe. Daraufhin wurde der Laptop gesperrt. Es ist nicht klar, aber andere Mitarbeiter haben möglicherweise dieselbe E-Mail erhalten.

In diesem Anwendungsfall gehören zu den potenziellen Problemen, die sich aus mangelnder Transparenz ergeben, dass es keinen Einblick in andere Mitarbeiter gibt, die dieselbe E-Mail erhalten haben, keine aktualisierte Ansicht der aktuellen Patchabdeckung, keine Kenntnis darüber, wer Administrationsrechte für Rechner hat, und keinen Einblick in die Anzahl der infizierten Geräte und deren Status.

Eine von Ivanti gesponserte Windows 10-Studie aus dem Jahr 2019 ergab, dass eines der größten Sicherheitsbedenken der Befragten das Risiko von Datenschutzverstößen ist (41 %), gefolgt von der Angst vor Ransomware/Malware (20 %). Darüber hinaus ergab eine weitere von Ivanti gesponserte Studie vom April 2019, dass 70 % der Unternehmen vor allem am Sicherheitsstatus interessiert wären, wenn sie Einblicke in Echtzeit erhalten könnten, und fast 60 % würden sich Einblicke in Anwendungsdaten wünschen.

Aus der Perspektive des Unified Endpoint Management erhöht ein Mangel an Transparenz den Zeitaufwand für die Bewältigung von Sicherheitsvorfällen. Außerdem nimmt das Risiko zu, dass sich ein Incident zu einem Sicherheitsvorfall entwickelt, der die Daten eines Unternehmens gefährdet, den Druck auf überlastete Teams erhöht und das Vertrauen in das Unternehmen schädigt. Die Ursache hierfür kann eingeschränkte Transparenz oder das Fehlen von integrierten Daten sein. Dies hat wiederum Widersprüche in Assetdaten und Sicherheitsinformationen zur Folge, durch die Transparenzlücken entstehen und schnelles Handeln erschwert wird.

Ist dagegen die Einsichtnahme in genaue Patchdaten und Nutzerzugriffsinformationen möglich, kann schneller auf Angriffe reagiert und das Netzwerk geschützt werden. Bedrohungen wie Lösegeldforderungen können abgewehrt und ihre Ausbreitung verhindert werden. Außerdem können Vorsichtsmaßnahmen für künftige Angriffe getroffen werden.

Ein Mangel an Transparenz erschwert obendrein die effiziente Verwaltung von Re-Imaging-Anforderungen zur Unterstützung von Abhilfemaßnahmen in den oben beschriebenen Situationen.

Umfassende Transparenz, welche Assets sich wo in der Umgebung befinden und wer sie wie nutzt, ganz ohne umständliche Arbeitsblätter, ist für die Mitarbeiter des Servicedesks entscheidend, damit sie ihre Arbeit effizient und mit kürzeren Lösungszeiten für Incidents und Probleme erledigen können. In diesem Anwendungsfall fördert die Verbesserung der Sichtbarkeit der potenziellen Bedrohung, die von der verdächtigen E-Mail ausgeht, eine schnellere Behebung.

6 Ins Unbekannte der IT-Umgebung

Eine IT-Analystin bewertet die Sicherheit der Umgebung und stellt dabei fest, dass nicht bekannt ist, welche Computer sich in der Umgebung befinden oder ob sie ordnungsgemäß verwaltet werden. Nur 75 % der Umgebung sind bekannt. Durch Aktualisierungen und Ähnliches sind Computer nicht länger verwaltet. Auf der Serverseite wurden virtuelle Maschinen ohne die richtigen Konfigurations-informationen erstellt und auch nicht mit den aktuellsten Patches auf dem neuesten Stand gehalten.

In diesem Anwendungsfall gibt es keine Sicht auf Endpunkte und Server der Umgebung und daher keinen Einblick in das, was auf Produktionsebene gepatcht wird. Zu wissen, wo all die physischen und virtuellen Assets des Unternehmen sind, ist nicht nur aus der Sicht von Service und Support entscheidend, sondern auch unter dem Aspekt der Sicherheit. Nicht verwaltete und nicht gepatchte Assets werden zum Risiko für Integrität und Compliance. Und mit der Zunahme von IT-Schwachstellen wird es immer wichtiger, den Überblick über jedes Gerät zu behalten.

Das zuvor bereits erwähnt Whitepaper von EY mit dem Titel „Data Validation the Best Practice for Data Quality in Fixed Asset Management“ (Datenvalidierung – Best Practice für Datenqualität bei der Verwaltung von Anlagevermögen) führt aus, dass 30 % der IT-Anlagegüter nicht auffindbare „Phantom“-Assets“ sind. Die Sichtbarkeit von Assets ist ein kritischer erster Schritt, da viele Unternehmen unterschätzen, was sie haben. Wenn sich Unternehmen erstmals mit dem IT-Assetmanagement auseinandersetzen, ist es nicht ungewöhnlich, 20 bis 30 % mehr Geräte zu finden, als sie zu haben glaubten. Sie können etwas, von dem Sie gar nicht wissen, dass Sie es haben, nicht verwalten, und dies stellt ein erhebliches Sicherheitsrisiko dar.

Mit Unified Endpoint Management-Lösungen erhalten Sie vollständige Transparenz und Kontrolle über Ihre Endgeräte. So können Sie alles schützen und Bedrohungen vermeiden, die von ungeschützten und nicht verwalteten Geräten ausgehen. IT-Teams profitieren von einer automatisierten Bereitstellungsstrategie, die Echtzeit-Scans durchführt und Nutzer- und Standortinformationen abgleicht. Zur Vermeidung einer unkontrollierte Ausbreitung virtueller Server ist es wichtig, dass Sie sehen können, wer über Administratorrechte verfügt, damit andere IT-Gruppen virtuelle Maschinen nur dann hochfahren können, wenn deren Sicherheit auf Höhe der Produktionsebene ist. Selbst in diesem Fall wird die Fähigkeit, diese neuen Server zu finden und sie zu Gruppen hinzuzufügen, verhindern, dass das nächste Wartungsfenster verpasst wird.

Darüber hinaus ist es sehr wichtig, dass Assets während ihres gesamten Lebenszyklus verwaltet werden. Durch die Verfolgung von Assetdaten, Problemen, Korrekturen, Patchinformationen, Verträgen und Lizenzierung können Sie dafür sorgen, dass Software- und Hardwareinvestitionen mit optimaler Leistung arbeiten und die Produktivität der Mitarbeiter nicht beeinträchtigt wird.

Ivanti: Die Augen im Hinterkopf

CIOs, CISOs und VPs der IT-Branche erreichen solche Führungs- und Verantwortungsebenen nicht, wenn sie zyklopisch oder kurzsichtig sind. In dieser Hinsicht kann die erweiterte Transparenz, die Ihnen unsere Unified Endpoint Management- und Enterprise Service Management-Lösungen eröffnen, Ihre Teamziele, Ihr Branchenwissen sowie Ihre Geschäftsziele und -visionen ergänzen und unterstützen.

Überzeugen Sie sich selbst davon, wie Ivanti Ihre IT-Transparenz verbessert und Sie in die Lage versetzt, entschlossen auf ein verbessertes IT-Erlebnis für die Nutzer hinzuarbeiten und Gewinne bei der organisatorischen Effizienz und Produktivität zu erzielen. Bitte kontaktieren Sie uns, um mehr zu erfahren.

ivanti

ivanti.de
contact@ivanti.de