SBT Small Biz Thoughts
von Karl W. Palachuk

DER SCHNELLSTE WEG ZU BESSERER PRODUKTIVITÄT FÜR IT-, HELPDESK- UND MSP-TEAMS

E-Book im Auftrag von Acronis

INHALT

Der schnellste Weg zu besserer Produktivität für IT-, Helpdesk- und MSP-Teams 3

Hoch lebe die API – die guten und die schlechten Seiten 4

Die Flut an Tools und ihre Folgen 5

Wir haben die gut integrierte Lösung 6

Der Reifegrad eines Unternehmens ist entscheidend 8

Investition in den Stack 9

Zusammenfassung und Fazit 10

Referenzen 11

Weitere Ressourcen 12

DER SCHNELLSTE WEG ZU BESSERER PRODUKTIVITÄT FÜR IT-, HELPDESK- UND MSP-TEAMS

von Karl W. Palachuk

Im Dezember 2019 hob Boeings Raumfahrzeug Starliner zu einem Rendezvous mit der internationalen Raumstation ISS ab. Der Auftrag war eigentlich einfach: erfolgreich starten, an der Internationalen Raumstation andocken und sicher zur Erde zurückkehren.

55 Minuten nach dem Start meldete die NASA eine „außerplanmäßige Zündung“, sodass sich der Starliner im falschen Orbit befand.

Sie hatten die Internationale Raumstation verfehlt. Komplett vorbei! Zum Glück war die Mission ein unbemannter Testflug.

Wie war eine solche Panne in dieser Welt der absoluten Präzision möglich? Ganz einfach: Die Kommunikation zwischen zwei unterschiedlichen Softwaresystemen verlief fehlerhaft. Es wurde zwar alles für eine offene, fehlerlose Kommunikation getan, doch trotzdem gab es einen Fehler: Die Borduhr war auf die falsche Zeit eingestellt, sodass das Raumfahrzeug nicht an der Stelle war, wo es zu einem bestimmten Zeitpunkt hätte sein sollen.

Führen wir uns das noch einmal genau vor Augen: NASA, SpaceX und Boeing verpflichteten sich einer zu einer partnerschaftlichen und offenen Zusammenarbeit. Jede Seite verfolgte gute Absichten und alle hatten die gleichen Ziele. Alle zogen an einem Strang und wollten das Gleiche erreichen.

Insgesamt gab Boeing 1,5 Milliarden US-Dollar dafür aus – und verfehlte das Ziel.

Daraus lassen sich Schlussfolgerungen über das Verhältnis zwischen Komplexität, Vernetzung und effizientem Einsatz von Software ziehen. Selbst wenn sich die Kooperationspartner auf Konstruktionsvorgaben einigen und ein Produkt auf komplett offenen, sorgfältig dokumentierten Plattformen entwickeln, kann immer noch etwas schiefgehen.

Nun stellen Sie sich eine Umgebung vor, in der die Entwickler nicht miteinander kooperieren, sondern im Wettbewerb zueinander stehen. Jeder veröffentlicht Spezifikationen über die Verbindung mit der eigenen Anwendungsschnittstelle (API), aber keiner kommuniziert direkt mit dem anderen.

Das Endprodukt erfüllt dann genau die Erwartungen: Es ist kompliziert, schlecht optimiert und störanfällig.

HOCH LEBE DIE API – DIE GUTEN UND DIE SCHLECHTEN SEITEN

Technologie entwickelt sich rasant. Während andere Branchen alle 10 Jahre eine Innovation erleben, gibt es in der IT alle 18 bis 24 Monate eine neue Technologiegeneration. Wenn Sie Ihre Abläufe seit fünf Jahren nicht verändert haben, sind sie längst veraltet.

Wir leben heute in einer Zeit, die von APIs geprägt ist. Sie wurden in den frühen 2000ern entwickelt und sollten die Zusammenarbeit, den Informationsaustausch und die Prozessautomatisierung zwischen mehreren Anwendungen erleichtern.

APIs waren für viele Managed Service Provider eine perfekte Ergänzung, da sie die Zusammenarbeit verschiedenster Tools möglich machten. Naturgemäß stiegen durch API-Middleware auch die Kosten für die Bereitstellung von Services. In einigen Fällen war die Middleware vergleichsweise teuer und dazu oft noch ziemliche Flickschusterei – aber sie funktionierte!

Aus der einst wunderbaren neuen Strategie war ein Baukasten geworden, mit dem jeder sein eigenes Frankensteinmonster basteln konnte.

Zurück zur Gegenwart. APIs sind heute zwar sehr ausgereift, allerdings müssen ihre Verbindungen auch unter den besten Bedingungen und der besten Programmierung immer noch verwaltet werden. Bei der Verbindung der Software zweier unterschiedlicher Unternehmen kann eine Änderung – egal auf welcher Seite – zu Funktionsstörungen führen. Ist zusätzlich eine Drittanbieterverbindung dazwischen geschaltet, wird es noch komplizierter.

Jede Verbindung benötigt einen gewissen Mindestaufwand an Verwaltung und birgt zudem ein potenzielles Sicherheitsrisiko, das überwacht werden muss. Ransomware ist derzeit ein Riesengeschäft und Cyberkriminelle haben entdeckt, dass IT-Service Provider wahre Fundgruben für Datendiebstahl und die Verbreitung von Schadcode sind. Wie bei jedem Angriff können sich die Angreifer dabei einen Eintrittspunkt aussuchen und darauf einhämmern. Deshalb muss jeder mögliche Angriffspunkt geschützt werden.

Ein ungeschriebenes Gesetz in der Software-Entwicklung lautet, dass Wartung und Support letztendlich immer mehr kosten als die Software selbst. (Als IT-Service Provider wissen wir das, weil wir unser Geld mit Support-Dienstleistungen verdienen.) Darüber hinaus steigt mit der zunehmenden Zahl an Verbindungen auch der Bedarf an Überwachung, Wartung und Support.

DIE FLUT AN TOOLS UND IHRE FOLGEN

Zusätzlich zu den Kosten für eine Vielzahl an Tools führt diese „Flut“ auch zu höheren Kosten für Schulung, Integration und Wartung. Eine Gartner-Studie hat gezeigt, dass Tool-Komplexität an mehreren Stellen zu höheren Ausgaben führt. Letzten Endes müssen wir uns eingestehen, dass APIs zwar unterschiedliche Software-Anwendungen miteinander verbinden, dabei jedoch ineffizient vorgehen. Mit jeder Verbindung nimmt die Komplexität zu und es kommen Dokumentation, Schulungen sowie zwei zusätzliche Verbindungen hinzu, die überwacht werden müssen.

Der Aufwand für die Wartung eines komplexen und vernetzten Systems beeinträchtigt auch die Produktivität insgesamt – jede Stunde, die für die Systemwartung aufgewendet wird, fehlt beim Support für die Endbenutzer.

Forrester Research fand in einer aktuellen Studie heraus, dass die Abhängigkeit von veralteten Toolsets eine der größten Hürden für die Modernisierung und digitale Transformation darstellt. Dabei stellten sie fest, dass 86 % der Unternehmen mindestens ein veraltetes Tool und nur 12 % vollständig integrierte moderne Überwachungstools einsetzen.

Diese Abhängigkeit von überholten und schlecht vernetzten Tools führt zu höheren Kosten für die Unterstützung der Umgebung, einer schlechteren Servicequalität und größeren Sicherheitsrisiken (mehr darüber siehe unten). Ein weiterer Nachteil beim Einsatz mehrerer Tools ist die Integration. Fast die Hälfte (46 %) aller Unternehmen gab an, „zu viel Zeit und Geld für die Wartung und Integration der verschiedenen Sicherheitsprotokolle jedes einzelnen Tools aufzuwenden.“

Dazu kommt außerdem, dass sich die Funktionen mehrerer Tools überlappen – dadurch bezahlen Sie zwei oder drei Mal für die gleichen Funktionen. In jedem Fall nutzt mindestens ein Tool nicht alle seine integrierten Funktionen, da es bereits eine ähnliche Funktion aus einem anderen Tool verwendet. Diese überlappenden Funktionen führen zu Komplexität, einem Mangel an Ressourcen und zusätzlichem Aufwand, der durch die Verwaltung mehrerer Tools entsteht.

> Kurz gesagt, verwenden die meisten Unternehmen eine Vielzahl von Tools, die schon von vornherein nicht gut vernetzt sind. Sie investieren in Tools mit doppelten Funktionen und müssen somit mehr Geld für Wartung und Lizenzen ausgeben. Für den laufenden Betrieb kommen mit jedem Toolset zusätzliche Schulungen, Dokumentation und Überwachung hinzu.
>
> Doch es geht auch anders.

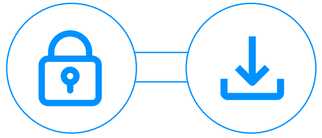
WIR HABEN DIE GUT INTEGRIERTE LÖSUNG

Die umständlichen APIs von früher sind Geschichte. Immer mehr IT-Teams entscheiden sich für Software-Lösungen, die schon ab Werk integriert sind und nicht erst im Nachhinein zusammengeschustert werden müssen. Wir bewegen uns weg von einer Welt, die von API-Übersetzungen beherrscht wird.

Komplexität spielt bei der Entwicklung und Wartung von Software eine wichtige Rolle und führt – wie zu erwarten – zu höheren Kosten für Wartung, Sicherheit und Support. Wenn

Beispiel Eins

Mit zwei Softwarelösungen und einem Connector haben Sie möglicherweise einen, zwei oder drei Partner, mit denen Sie zusammenarbeiten müssen. Jeder von ihnen könnte eine Änderung vornehmen, die entweder zum Abbruch der Verbindung führt oder eine neue Schwachstelle verursacht, die ausgenutzt werden könnte.



Beispiel Zwei

Mit drei Softwarelösungen und zwei Verbindungsgliedern haben Sie möglicherweise einen, zwei, drei, vier oder fünf Partner, mit denen Sie zusammenarbeiten müssen. Jeder von ihnen könnte wieder eine Änderung vornehmen, die entweder zum Abbruch der Verbindung führt oder eine neue Schwachstelle verursacht, die ausgenutzt werden könnte.

Beispiel Drei

Werfen wir einen Blick auf die jetzt neu aufkommende, „integrierte“ Welt der Sicherheitsanwendungen. Diese Anwendungen sind von Anfang an für die Zusammenarbeit konzipiert und wurden alle vom gleichen Team entwickelt.

Sie je ein separates System für Backup, Malware-Schutz, Remote-Desktop-Support und Verwaltung haben, gibt es bei Ihnen auch viele Verbindungen. Jede dieser Verbindungen hat mehrere Schwachpunkte und mögliche Bedrohungsvektoren innerhalb Ihrer Umgebung.

Nehmen wir an, Sie möchten zwei Anwendungen und deren Services (z. B. Backup und Virenschutz) miteinander verbinden. Für die Umsetzung gibt es verschiedene Möglichkeiten. Wurden sie vom selben Unternehmen entwickelt? Sind sie von Anfang an auf Zusammenarbeit ausgelegt? Falls es eine Verbindung zwischen beiden Systemen gibt: Wurde diese von einem der ursprünglichen oder einem separaten Unternehmen geschrieben?

Je geringer die Komplexität der Software, desto mehr Vorteile haben Sie: höhere Effizienz und Produktivität, weniger Wartungsaufwand sowie mehr Sicherheit. Zudem sparen Sie von Anfang an Kosten, da Sie keine Ausgaben für Drittanbieter-Middleware haben, die Ihre Anwendungen untereinander verbindet. Und Sie sparen Zeit für die Administration und Verwaltung zusätzlicher Anwendungen.

Ein zunehmendes Problem unter IT-Service Providern ist Vendor Fatigue (Anbietermüdigkeit). Das bedeutet, die Mitarbeiter werden mit Rechnungen von Unternehmen überflutet, die dafür sorgen, dass alles so funktioniert, wie es soll.

Ein Unternehmen geht dieses Problem direkt an. Acronis hat ein Paket an Produkten entwickelt, die nahtlos zusammenarbeiten. Acronis Cyber Protect wurde von Grund auf neu konzipiert und maximiert die Effizienz, indem Komplexität und Gesamtbetriebskosten (TCO) verringert werden. Acronis Product Marketing Manager Lauren Beliveau betont: „Wir haben nicht nur eine Reihe von Produkten – wir haben ein Paket voller Lösungen.“

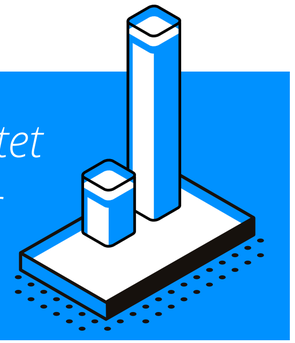
Es geht hier nicht nur um ein theoretisches Problem. In der Sicherheitswelt stellt dieser „Flickenteppich“ aus veralteten Tools eine ernste Bedrohung dar, die zusätzlich überwacht werden muss. Jede Verbindung steht für eine potenzielle Schwachstelle – ebenso wie jeder Patch und jedes Update. Patches müssen nicht nur angewendet werden; anschließend muss auch überwacht werden, ob eventuell Probleme entstanden sind. In einigen Fällen muss der Patch entfernt und wieder neu installiert werden, sobald neue Schwachstellen auftauchen.

Leider warten viele Unternehmen vor der Anwendung von Patches eine gewisse Zeit, um sicherzugehen, dass diese keine zusätzlichen Probleme, Inkompatibilitäten oder Schwachstellen verursachen. Das führt dazu, dass Anwendungen für längere Zeit gegenüber bekannten Schwachstellen anfällig sind.

Darüber hinaus nutzen schlecht integrierte Anwendungen von verschiedenen Anbietern nicht immer gemeinsam Daten, Warnmeldungen, Automatisierung, Dokumentation, Benutzeroberflächen, Agenten und anderes. Jede Schwachstelle in einer Verbindung ist auch eine Schwachstelle in der Sicherheit. Heutzutage ist das Risiko solcher Schwachstellen einfach zu groß, um ignoriert zu werden.

Dank Acronis Cyber Protect weiß der Virenschutz, dass ein Backup existiert und scannt es. Mit einer vollständig integrierten Lösung arbeiten Tools wie Backup und Virenschutz effizienter zusammen. Backups werden automatisch auf Bedrohungen (z. B. Viren, Malware und Ransomware) untersucht, um sicherzustellen, dass die Daten sauber sind. Patches werden auf Backups und aktiv laufenden Systemen angewendet. All dies passiert buchstäblich nahtlos.

Geringere Komplexität der Software bedeutet höhere Effizienz und Produktivität, weniger Wartungsaufwand sowie mehr Sicherheit.



DER REIFEGRAD EINES UNTERNEHMENS IST ENTSCHEIDEND

Ein weiterer Faktor, der selten in Betracht gezogen wird, ist der Reifegrad des Unternehmens, das die Tools entwickelt. In der Entwicklung vom Startup zum Großunternehmen durchlaufen Firmen mehrere Phasen. Am Anfang existiert ein unreifes Produkt mit nur einer Funktion (z. B. Virenschutz) und entfaltet im Laufe der Zeit seine vollen Funktionen. Beim Übergang vom Startup zum etablierten Unternehmen liegt der Schwerpunkt darin, das Produkt auf den Markt zu bringen und vielleicht sogar Geld damit zu verdienen.

Etablierte Startups konzentrieren sich auf die Entwicklung weiterer Funktionen und Verbindungsmöglichkeiten und nutzen dazu die allmächtigen APIs. In dieser Phase besteht das Ziel darin, sich mit allen zu verbinden. Hier geschieht vielleicht die meiste Flickschusterei. In den meisten Fällen funktioniert das, nur sind die APIs nicht ausgereift und alles verändert sich ständig. Stellt sich Erfolg ein, fordern die Anwender mehr Funktionen – also wird zur nächsten Phase übergegangen: die Vergrößerung der Anwenderbasis.

Unternehmen, die ihre Basis vergrößern möchten, sind auch am Kauf oder an der Entwicklung neuer Funktionen interessiert. In dieser Phase besteht die Strategie darin, durch mehr Funktionen und die Zusammenarbeit mit mehr Wettbewerbern mehr Kunden zu gewinnen. Letztendlich gilt es, Marktanteile zu erobern, indem man auf Anwenderforderungen eingeht und ein vielseitigeres Toolset entwickelt. Diese Phase der Expansion ist auch geprägt durch große interne Veränderungen und die ständige Bemühung, mit den sich entwickelnden APIs mitzuhalten – sowohl intern bei der Verbindung gekaufter und zu integrierender Produkte als auch bei der Verbindung eigener und Mitbewerber-Produkte.

In der nächsten Phase geht es um die finanzielle Expansion. Ab einem bestimmten Punkt benötigen Unternehmen Geld in Form von Risikokapital oder anderen Finanzierungsquellen, um expandieren zu können. Dies wiederum führt dazu, dass auf Kundenanfragen nicht mehr so schnell reagiert werden kann. Das Management verlegt den Fokus von Funktionalität auf Finanzen und folglich wird der Umsatz wichtiger als die Behebung von Problemen oder Entwicklung neuer Funktionen.

Dies war im Laufe der Jahre bei Fusionen zu beobachten: Besonders konstruktive und flexible Anbieter beheben plötzlich keine Probleme mehr und die Produkt-Roadmap wird für die IT-Spezialisten, die auf die Software angewiesen sind, sehr undurchsichtig. Jetzt ist alle Aktivität im Unternehmen nur noch auf Umsatz ausgerichtet, während die Entwicklung (einschließlich Problembehebung) deutlich reduziert wird.

Nur einige wenige Unternehmen leben lang genug, um wirklich reifen zu können und gut integrierte Tools zu entwickeln, die nahtlos zusammenarbeiten und zudem ausreichende

Unterstützung auf der programmiertechnischen Seite haben, um neue Funktionen hinzuzufügen, ohne andere Funktionen zu beeinträchtigen oder neue Probleme zu erzeugen. Neben den technischen Herausforderungen haben ausgereifte Unternehmen gelernt, langfristig in die stetige Entwicklung sowie in Vertrieb und Kundensupport zu investieren.

Da sich die Technologie von Jahr zu Jahr schneller verändert, werden neue Funktionen für die Bewältigung neuer Herausforderungen benötigt. Das gilt bei Cybersicherheit noch mehr als in allen anderen Bereichen. Vor zehn Jahren waren Viren nur lästig und zerstörerisch. Heute können sie mehrere Millionen an Kosten für Lösegeld verursachen, zusätzlich zu den Kosten für Ausfallzeiten.

Weniger ausgereifte und von Fusionen und Übernahmen geprägte Unternehmen halten an älteren Produkten fest. Sie haben oftmals nicht die Zeit bzw. das Geld oder sind intern nicht darauf ausgerichtet, mit den Anforderungen eines sich stetig weiterentwickelnden Sicherheitsumfelds mitzuhalten.

Im besten Fall verwenden sie alte Lösungen – im schlimmsten Fall sind ihre Lösungen nicht mit neueren Tools kompatibel.

Mit zunehmender Komplexität des Toolsets verringert sich die Effizienz. Zusätzlich zu den Problemen, die der Einsatz mehrerer APIs mit sich bringt, müssen auch die unterschiedlich ausgereiften inneren Bestandteile der Software, der Support durch Firmen mit unterschiedlich ausgereiften APIs und außerdem noch die Dokumentation gemanagt werden.

Das Gesamtpaket sollte das bestmögliche sein. In einigen Fällen bedeutet das, nach den besten Lösungen ihrer jeweiligen Klasse zu suchen, auch wenn sie von verschiedenen Anbietern stammen. Doch nach Möglichkeit sollten all diese Lösungen von einem einzigen Anbieter kommen, um die Effizienz und Sicherheit zu steigern und die damit zusammenhängenden Kosten zu senken.

> Mit Acronis Cyber Protect erhalten Sie das Beste aus beiden Welten. Acronis gilt weithin als der führende Anbieter für Data Protection und Recovery. Das Unternehmen bietet eine ganze Sammlung erstklassiger Lösungen für die Sicherung von Daten, Applikationen und Systemen – ganz ohne störende Middleware.
>
> Acronis Cyber Protect umfasst konkurrenzlose Funktionen, zum Beispiel die Anwendung von Patches auf Backup-Images, womit verhindert wird, dass die Sicherheitsstufe von Client-Maschinen durch eine Wiederherstellung herabgesetzt wird.

Bei all den Problemen durch Ransomware, millionenschwere Klagen und behördliche Vorschriften sollten Sie in den kommenden Jahren Ihr Geld und Ihre Energie nicht für die Zusammenstellung von Sicherheitstools verschwenden und auf deren gute Zusammenarbeit hoffen. Sie benötigen Lösungen, die innovative Funktionalität und Sicherheit bieten – ohne die damit einhergehenden Nachteile wie Komplexität, Wartung und Kosten.

Entscheiden Sie sich für das einzige Sicherheitspaket, das für vollständige Integration konzipiert wurde.

ZUSAMMENFASSUNG UND FAZIT

Sicherheit darf nicht mehr als zusätzliche Funktion für andere Services betrachtet werden. In den kommenden Jahren müssen Technologieberatern grundsolide, allumfassende Lösungen zur Verfügung stehen, die unschlagbare Sicherheit bieten und gleichzeitig nicht die Produktivität der Anwender beeinträchtigen.

Komplexität verringert Effizienz und Produktivität, während die Kosten für Wartung, Dokumentation und Schulung steigen. Mit zunehmender Zahl an „Einzelteilen“ steigt auch die Zahl der Verbindungsglieder. Ein vollständig integriertes Paket, das für nahtlose Zusammenarbeit ausgelegt ist, erhöht die Sicherheit insgesamt und reduziert Komplexität sowie dadurch anfallende Kosten.

APIs wird es noch für längere Zeit geben. Zum Glück lassen sich komplexe vernetzte Systeme produktiver verwalten, wenn Sie über das vollständig integrierte Paket von Acronis verfügen, dem führenden Anbieter in Cyber Security und Data Protection.

Verbindungen sind gut – Integration „by design“ ist besser.

REFERENZEN

https://www.msn.com/en-us/news/technology/boeings-software-troubles-show-an-engineering-culture-clash/ar-BB16xEdq

https://www.forbes.com/sites/jonathanocallaghan/2019/12/20/boeing-starliner-spacecraft-launches-to-the-international-space-station-heralding-a-new-era-for-american-human-spaceflight/

If This Then That
https://ifttt.com/

Zapier
https://zapier.com/

Programmable Web
https://www.programmableweb.com/

Salesforce.com
www.salesforce.com

Harvard Business Review: „The Strategic Value of APIs“ (Der strategische Wert von APIs).
https://hbr.org/2015/01/the-strategic-value-of-apis

„Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices“ (Laut Gartner können Unternehmen ihre Softwarekosten mit drei Best Practices um 30 Prozent senken)
https://www.gartner.com/en/newsroom/press-releases/2016-07-19-gartner-says-organizations-can-cut-software-costs-by-30-percent-using-three-best-practices

Forrester Research: „Prevalence Of Legacy Tools Paralyzes Enterprises' Ability To Innovate“ (Veraltete Tools bremsen die Innovationsfähigkeit von Unternehmen)
https://sciencelogic.com/wp-content/uploads/sciencelogic-os.pdf

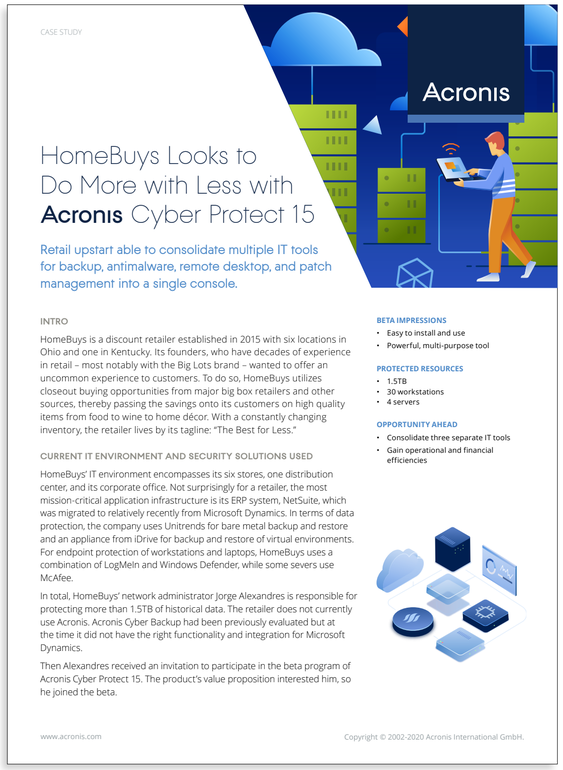
„Struggling With Toolchain Sprawl? You're Not Alone“ (Sie kämpfen mit zu vielen Tools? Sie sind nicht allein!)
https://dzone.com/articles/toolchain-sprawl-youre-not-alone

INFORMATIONEN ZUM AUTOR

Karl W. Palachuk hat zwei Managed Services-Unternehmen in Sacramento, Kalifornien gegründet und verkauft. Er ist Gründer und Präsident der Sacramento SMB IT Professionals Group und Autor mehrerer Bücher, darunter „The Network Documentation Workbook“ und „Managed Services in a Month“.

Karl W. Palachuk ist seit 15 Jahren gefragter Referent bei Konferenzen und Seminaren auf der ganzen Welt. Er ist ein Microsoft Certified Systems Engineer mit einem Bachelor-Abschluss der Gonzaga University und einem Master-Abschluss der University of Michigan. Er ist außerdem Microsoft Small Business Specialist und Gründungsmitglied des Microsoft Small Business Specialist Advisory Panel.

WEITERE RESSOURCEN


CASE STUDY

Acronis

HomeBuys Looks to Do More with Less with **Acronis** Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: "The Best for Less."

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys' IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some severs use McAfee.

In total, HomeBuys' network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product's value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies

www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.

Acronis Blog: Liefert Ihnen die neuesten Updates und Einblicke des weltweit führenden Unternehmens für Cyber Protection.

Acronis YouTube-Kanal: Für regelmäßige Videos zu Anwendungsfällen, Demos, Analysen von Cyberbedrohungen und Neuigkeiten zum Unternehmen.

Acronis Ressourcencenter: Die erste Anlaufstelle für Whitepaper, E-Books, ausführliche Artikel, Tutorials, Infografiken u. a. zum Thema Cyber Protection.

Acronis Events: Laufende Veranstaltungsreihen, Webinare, Interviews u. a. und mehr darüber, wie Sie bei uns einsteigen können.

ÜBER ACRONIS

Acronis vereint Data Protection und Cyber Security in einer integrierten, automatisierten Cyber Protection-Lösung, die mit Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit (engl. safety, accessibility, privacy, authenticity, security, kurz: SAPAS) die Herausforderungen der modernen digitalen Welt bewältigt. Dank flexibler Deployment-Modelle, die die Anforderungen von Service Providern und IT-Verantwortlichen erfüllen, bietet Acronis hervorragende Cyber Protection für Daten, Applikationen und Systeme mit innovativen Lösungen, die Virenschutz der nächsten Generation, Backup, Disaster Recovery und Verwaltung für den Endpunktschutz umfassen. Unterstützt durch preisgekrönten KI-basierten Malware-Schutz und Blockchain-basierte Authentifizierung schützt Acronis Ihre Daten in allen lokalen, Cloud-basierten und hybriden Umgebungen – zu geringen und vorhersagbaren Kosten.

Acronis wurde 2003 in Singapur gegründet und ist seit 2008 in der Schweiz eingetragen. Heute beschäftigt das Unternehmen mehr als 1.500 Mitarbeiter an 33 Standorten in 18 Ländern. Den Acronis Lösungen vertrauen bereits mehr als 5,5 Millionen Privatanwender und 500.000 Unternehmen – einschließlich 100 % der Fortune 1000-Unternehmen und erstklassige Profisport-Teams. Acronis Produkte können über mehr als 50.000 Partner und Service Provider in über 150 Ländern und in mehr als 40 Sprachen erworben werden.

SBT Small Biz Thoughts

von Karl W. Palachuk

SmallBizThoughts.com

E-Book im Auftrag von **Acronis**

acronis.com