12 | 22 Sonderdruck für Deskcenter

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Markus Gärtner im Interview

www.it-administrator.de

»Transparenz ist wirklich das A und O«

Das Clientmanagement bereitet dem IT-Verantwortlichen stets neues Kopfzerbrechen. Themen wie Betriebssystem- und Softwareverteilung schienen technisch lösbar, doch Remote Work, eine Vielzahl neuer, teilweise persönlicher Endgeräte und das ewige Thema Sicherheit bescheren der IT neue Aufgaben. Wir sprachen mit Markus Gärtner, Vorstand bei der Deskcenter AG, über eine zeitgemäße Verwaltung der Endgeräte.

IT-Administrator: Welches sind Ihrer Erfahrung nach aktuell die größten Herausforderungen bei der Verwaltung der Endanwender-Rechner im Unternehmen – wenn wir die Security einmal außen vor lassen?

Markus Gärtner: Der Elefant im Raum ist die Transparenz. Sie steht hinter der Security und allen anderen Themen. Bevor überhaupt Maßnahmen ergriffen werden können, braucht es nämlich die richtigen Entscheidungen. Und diese lassen sich wiederum nur auf der Grundlage eines detaillierten und vollständigen Status quo treffen. Denn wollen IT-Verantwortliche Lizenzkosten sparen, müssen sie wissen, welche Programme überhaupt benutzt werden. Und wenn sie Apps auf mobile Endgeräte ausrollen, brauchen sie Daten, welche wo im Einsatz sind. In hybriden Landschaften ist es wichtig, unnötige Redundanzen zwischen Diensten in der Cloud und lokalen Installationen zu vermeiden. Transparenz ist wirklich das A und O.

Das ist ja nichts Neues. Warum tut sich hier nichts?

Am Willen der IT-Teams liegt es sicherlich nicht. Die arbeiten in der Regel von früh bis spät. Durch den Trend zu Remote Work ist die Arbeitslast sogar nochmals gestiegen. Da bleibt wenig bis gar keine Zeit für strategische Überlegungen, etwa zur Automatisierung in der IT – aber gerade die braucht es, damit sich etwas ändert. Die IT-Verantwortlichen müssen sich eingestehen, dass es so wie bisher nicht weitergehen kann und sind aufgefordert, endlich einen Business Case zusammenzustellen. Das ist kein Hexenwerk, die Vorteile lassen sich leicht aufzeigen. Nehmen wir nur das Beispiel Schwachstellenanalyse. Ist einmal entschieden, was in einem bestimmten Szenario zu tun ist, lässt sich der Lösungsansatz als Standard hinterlegen – inklusive eines automatisierten Ablaufplans, wie eine Sicherheitslücke zu beseitigen ist. Trifft ein anderer Mitarbeiter erneut auf diese Schwachstelle, etwa in einer neu installierten Software, läuft der Automatismus. So sparen IT-Abteilungen sowohl Mitarbeiterkosten als auch Reaktionszeit, um einer Cyberattacke vorzubeugen.

Und auf welche Maßnahmen beziehungsweise technischen Features eines Clientmanagements darf ein Unternehmen heutzutage keinesfalls mehr verzichten?

Ich sehe hier zwei zentrale Punkte: Zum einen ein automatisiertes Patching. Das muss aber wirklich umfänglich sein. Wer hier nur häufig eingesetzte Anwendungen wie von Microsoft und Adobe ins Visier nimmt, öffnet Angreifern Tür und Tor. Gepatcht werden müssen auch seltenere Apps und die vielen kleinen Helferprogramme, selbst wenn sie nur auf einzelnen Rechnern, Smartphones oder Tablets installiert sind. Zum zweiten ist es wichtig, Schwachstellen so früh wie möglich zu erkennen, selbst wenn es noch keinen Patch gibt.

> **»IT-Verantwortliche müssen sich eingestehen: So wie bisher kann es nicht weitergehen.«**

Warum sollten Unternehmen denn Zeit investieren in die Analyse von Lücken, für die es noch gar keine Patches gibt?

Weil wir uns in einem ständigen Wettlauf mit den Hackern befinden und ein neu bekannt gewordener Exploit manchmal innerhalb von Stunden genutzt wird – wie in der weit verbreiteten Java-Bibliothek Log4j, für den das BSI im Dezember 2021 Alarmstufe Rot ausrief. Hier braucht es einen automatisierten Warnservice, damit IT-Verantwortliche keine wertvolle Zeit verlieren, um betroffene Rechner vom Netz zu nehmen und in Quarantäne zu stecken. Neben Aspekten des Risikomanagements ist das auch eine versicherungstechnische Frage. Denn damit eine Cyberversicherung leistet, müssen Betroffene eine rasche, angemessene Reaktion nachweisen.

Gerade mobile Endanwender erwarten, dass sie die vollständige Kontrolle über ihr Gerät haben, was die IT nicht immer zulassen kann. Wie sieht Ihrer Ansicht nach hier der beste Kompromiss aus?

Das Handy empfinden Mitarbeitende als sehr persönliches Gerät, viel persönlicher als etwa den Firmenlaptop. Das macht es schwierig. Und leider gehen nötige Schutzmaßnahmen immer zu Lasten des Bedienkomforts. Mein Lieblingsbeispiel ist die Zweifaktor-Authentifizierung: Sie ist wirkungsvoll, allerdings sehr umständlich. Aber einen Kompromiss kann sich die IT heutzutage aus Sicherheitsgründen nicht mehr leisten. Gerade weil so viel passiert – und immer mehr in den Medien berichtet wird – lautet mein Tipp: Auf Aufklärung setzen! IT-Verantwortliche sollten ihre Belegschaft immer wieder über spektakuläre Fälle informieren. So werben sie um Verständnis für strenge Schutzmaßnahmen und als lästig und kleinkariert empfundene Vorschriften.

KMU haben ja nicht immer alle Geräte auf dem neuesten Hardwarestand und dieser ist zudem oft nicht homogen. Welche Probleme bringt dies mit sich und was raten Sie IT-Verantwortlichen?

Die Liste der Probleme ist wirklich sehr lang. Da wäre zunächst der immense Wartungs- und Supportaufwand, vom Ersatzteil bis hin zum Fachwissen für die Fehlerbehebung. Je nach installierter Software sind auch Freigaben anders einzurichten – was wiederum dazu führt, dass für Updates verschiedene Konstellationen zu testen sind. Veraltete Hardware oder Software lässt in der Regel keine weiteren Updates mehr zu und stellt damit ein Betriebsrisiko dar. Sollte mal wirklich etwas mit der Maschine sein – wer kennt sich da noch aus? Gleichzeitig ist es nicht nötig, dass alle Endanwender immer die neuste Hardware

verwenden, so brauchen Entwickler oder Konstrukteure meist leistungsstärkere Geräte als das Marketing oder die Buchhaltung. Die vielbeschworene Standardisierung ist also nicht immer wirtschaftlich. Besser ist es, ausgehend von einer umfassenden Inventarisierung, gezielt nach "low hanging fruits" zu suchen. Ich rate, in regelmäßigen Abständen zu prüfen, ob sich beim IT-Portfoliomanagement Optimierungspotenziale auftun.

Zudem gehört der Rechnerpark der Endanwender und dessen Support oft zu relativ teuren Teilen des IT-Betriebs. Wenn ein Unternehmen hier sparen will oder muss, was raten Sie?

Gerade bei kleinen und mittleren Unternehmen ist die IT-Abteilung oft chronisch unterbesetzt. Deshalb müssen die Supporter maximal unterstützt und entlastet werden. Von einer sinnvollen Standardisierung haben wir ja schon gesprochen. Unterstützung bietet auch eine Know-ledge Base, in der alle ihr Wissen und sämtliche Lösungsansätze dokumentieren und teilen. Wenn User über ein Self-Service-Portal einfache Probleme selbst lösen können und Bestellprozesse im Backend inklusive Freigaben automatisiert ablaufen, ist das ebenso eine große Entlastung – und sorgt gleichzeitig noch für Benutzerzufriedenheit. Kommt der Anwender nicht weiter und ruft an, ist es hilfreich, mit dem Call gleich alle Details zur Hardware, Software und aktuellen Leistungsparametern angezeigt zu bekommen. Das beschleunigt die Fehleranalyse, wie uns unsere Kunden immer wieder bestätigen.

Markus Gärtner

Auch ist die durchaus wünschenswerte regelmäßige Wartung von Endanwender-Rechnern für viele Unternehmen eine Herausforderung. Welche Vorgehensweise würden Sie IT-Verantwortlichen in diesem Umfeld anraten?

Die Herausforderung ist, das richtige Wartungsfenster zu finden – und, dass die User mitspielen und die Aufforderung zum Update nicht ständig wegklicken, weil sie lange Downtimes fürchten. Schon ziehen Tage oder Wochen bis zum Update ins Land. Hilfreich kann es da sein, das System den richtigen Zeitpunkt für das automatisierte Update wählen zu lassen – sei es während der Mittagspause, an Wochenenden oder nachts, wozu der Rechner dann automatisch hoch- und runtergefahren wird. Zur automatisierten Wartung gehören übrigens nicht nur das OS-Deployment und die Softwareverteilung. Auch unerlaubt installierte Apps wie Spiele lassen sich so aufspüren und automatisch deinstallieren.

Was sind Ihrer Ansicht nach die Vor- und Nachteile von Desktop-as-a-Service wie zum Beispiel beim Azure Virtual Desktop?

Für den kurzfristigen Bedarf kann dies interessant sein. Die Vorabkosten sind hier geringer als bei VDI oder klassischen Desktops. Allerdings muss der Standardisierungsgrad schon sehr hoch sein. Außerdem gibt die IT so die Kontrolle über Updates und Patches in fremde Hände. Zudem schützt die Cloud nicht vor dem Risiko, aus Versehen Daten zu löschen, eine Backupstrategie braucht es also dennoch.

Künstliche Intelligenz ist in aller Munde – auch im Clientmanagement?

Ja, absolut. Bots und Natural Language Processing sind da nur der erste Schritt. KI-Algorithmen werden zunehmend helfen, aus den riesigen Mengen an Bestands- und Zustandsdaten konkrete Handlungsempfehlungen abzuleiten. Dazu muss natürlich die Datenqualität stimmen. Denn die Auswertungen sind nicht aussagekräftig, wenn zum Beispiel für denselben Hersteller zig Schreibweisen existieren. Es braucht also auch einen automatisierten Normalisierungsprozess. Ist diese Klippe genommen, können KI-basierte Analysen einen höherer Erkenntnisgewinn und schnellere Handlungsempfehlungen liefern.

Wir danken für das Gespräch.