funkschau

All for One Steeb AG

Suchbegriff 1. All for One, -Steeb AG

Verlag WEKA FACHMEDIEN GmbH, URL: www.weka-fachmedien.de
Redaktion funkschau Redaktion, Tel.: 089 25556 1000, E-Mail: redaktion@funkschau.de

Ausgabe 08.12.2017 • Nr. 23-24/2017
Seite 14
Rubrik

Medientyp Fachpresse
Erscheinungsweise 2 x monatlich
Branche Telekommunikation allgemein
Bundesland Überregional

Publikation	verkauft	verbreitet	gedruckt	Reichweite Mio	Medien-Nr.
funkschau	5.477	35.543	36.000	0,20	2670

ARGUS DATA INSIGHTS® Deutschland GmbH
Gneisenaustr. 66, 10961 Berlin | T +49 30 203 987-0 | F +49 30 203 987-77 | E sales@argusdatainsights.de | www.argusdatainsights.de

UNTERSCHÄTZTE ERP-SICHERHEIT

Ein veraltetes ERP-System kann zum Unternehmensrisiko werden. Firmen sollten Schwachstellen ernst nehmen und zügig handeln.

Autor: Matthias Weber **Redaktion: Sabine Narloch**

➤ Ob moderne Betriebsabläufe, die wachsende Mobilität oder Datenmassen, die sich kaum handhaben lassen: Diese Faktoren bewegen Software-Hersteller dazu, schneller als jemals zuvor neue Funktionen auf den Markt zu bringen. Doch wie reagieren Firmen auf diese stark verkürzten Entwicklungszyklen? Kaum! Denn wer trennt sich von einem vertrauten System, das über Dekaden den Arbeitsalltag begleitet hat? Zudem ist es für IT-Verantwortliche schwer, regelmässig neue Investitionen zu rechtfertigen.

Diese Bequemlichkeit und finanzielle Zurückhaltung hat Folgen. Neben ineffizienten Betriebsabläufen und schwindender Wettbewerbsfähigkeit führt das Verhalten zu einem erhöhten Sicherheitsrisiko. Besonders unterschätzt wird das ERP-System, wie die Konferenz Black Hat Europe Ende 2015 demonstrierte: Experten haben ERP-Anwendungen eines Ölkonzerns angegriffen, um den Pipeline-Druck zu manipulieren. Dieses Szenario wirft bei vielen Firmen Fragen auf. Zum Beispiel, wo ihre eigenen Schwachstellen liegen und was man dagegen tun kann.

Schwachstelle ERP-System

Gerade im Mittelstand setzen viele Unternehmen seit Jahrzehnten auf das gleiche ERP-System. Wer hier aus Kostengründen auf die Softwarepflege verzichtet, arbeitet häufig mit einer veralteten Technologie, die einen Angriff erleichtert. Hinzu kommen weitere Probleme:

➤ Fehlende Kompatibilität: Veraltete Software lässt sich nicht zwingend mit anderen, neueren Programmen verbinden. Auch Herausforderungen mit Servern und Browsern können auftreten. Kritisch wird es, wenn das komplette Programm oder bestimmte Features nicht mehr unterstützt werden. Dann entfallen sowohl Support bei möglichen Störungen als auch die wichtigen Sicherheitsupdates.

➤ Fehlende Verschlüsselung: Gerade im E-Commerce braucht es innerhalb und außerhalb des Kundennetzes passende Schnittstellen, die eine Brücke zwischen dem Unternehmen und Marktplätzen wie Amazon und Ebay schlagen. „Diese Schnittstellen sind immer auch kritische Angriffspunkte", sagt Axel Krämer, Leiter Abteilung Central Services bei der All for One Steeb AG. „Als Beispiel ist der Zugriff auf ERP-Systeme via SSL-verschlüsselte Kommunikationsschnittstellen zu nennen. Wenn hier nicht die aktuellste Verschlüsselungstechnologie verwendet wird, hat das System eine ernstzunehmende Schwachstelle und bietet Raum für Datendiebstahl."

➤ Fehlendes Zugriffsreglement: Mit zum Teil großem Engagement widmen sich Unternehmen beim IT-Risikomanagement externen Bedrohungen und der Endnutzersicherheit. Was dabei allerdings zu kurz kommt, ist die Verteilung der Zugriffsrechte. Es braucht Steuerungsmechanismen, die es nur bestimmten Personen erlauben, Programmänderungen vorzunehmen. Oft wird auch der Nutzer unterschätzt, der zum Beispiel Kreditlimit-Prüfungen deaktiviert und damit

GUIDELINE FÜR MEHR SICHERHEIT

1. SCHWACHSTELLEN IDENTIFIZIEREN:

Bei der Prüfung des ERP-Systems sollten im ersten Schritt alle möglichen Schwachstellen bestimmt werden. Diese Liste sollte nach Dringlichkeit priorisiert werden. Dabei ist auch eine Aufwands- und Kostenschätzung abzugeben, die gerade bei der Besprechung mit den Budgetverantwortlichen helfen kann.

2. SICHERHEITSZIELE DEFINIEREN:

Basierend auf der Vorarbeit gilt es nun, die Sicherheitsziele für das ERP-System zu entwickeln. Erst die Analyse des Status quo hilft dabei, Handlungsfelder und die damit verbundenen Ziele zu evaluieren. Hinzu kommen noch die unternehmensweiten IT-Ziele.

3. ZUGANGSBERECHTIGUNGEN FESTLEGEN:

Gerade für das ERP-System braucht es klare Zugriffsregeln. Begrenzen Sie unbedingt die Anzahl der Mitarbeiter, die mit dem System arbeiten müssen, auf das Nötigste. Zudem ist zu analysieren, wer welche Berechtigung braucht. Dafür ist der nächste Schritt hilfreich.

4. ANWENDERGRUPPEN ANLEGEN:

Über die Erstellung von Tätigkeitsprofilen lässt sich ableiten, wer welche Funktion nutzen darf. Auch die Mitarbeiterposition sollte bei der Rechtevergabe beachtet werden. Der Abteilungsleiter benötigt den Zugriff auf andere Daten als der Mitarbeiter. Ziel ist es also, Zugänge nach den Tätigkeitsprofilen und nach Mitarbeiter zu verteilen.

5. PROZESSE AUFSETZEN:

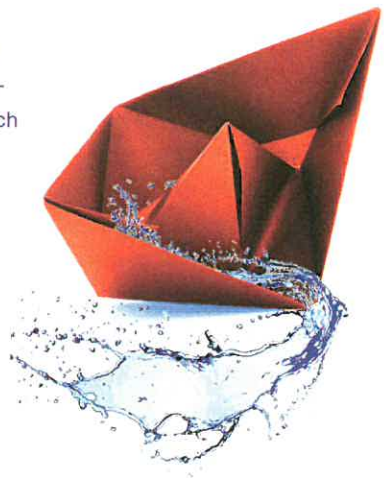
Sollte ein Mitarbeiter das Unternehmen verlassen, braucht es eine Schnittstelle zwischen IT- und HR-Abteilung. Oft genügt schon eine simple Information mit dem Namen des Ausscheidenden und der Bitte, alle Zugriffsrechte zu entziehen. Gerade im Cloud-Umfeld ist das essenziell, da hier Mitarbeiter mit ihrem eigenem Rechner arbeiten und nicht Teil des Firmennetzwerkes sind. Darüber hinaus sollten regelmäßig, mindestens jährlich, die Zugriffsregeln überwacht werden.

6. UPDATES UND TESTS DURCHFÜHREN:

Kontinuierliche Aktualisierungen und Sicherheitsupdates sind Pflicht. Das gilt für die Anwendung selbst, aber auch für alle Programme wie die entsprechende Firewall und das Betriebssystem, auf dem die ERP-Lösung läuft. Auch Tests müssen durchgeführt werden. In sogenannten Penetrationstests versetzen sich IT-Experten in die Rolle von Hackern und prüfen das ERP-System auf Schwachstellen. Anschließend halten sie ihre Ergebnisse in einem Bericht fest.

7. SCHULUNGEN UMSETZEN:

Da viele Mitarbeiter sich nicht umfänglich über die Gefahren im Klaren sind, sollten Firmen regelmäßige Schulungen abhalten und für das Thema IT-Sicherheit sensibilisieren – und zwar alle Mitarbeiter, auch die Chefetage.



Aufträge ohne Prüfung freigibt. Das kann im schlimmsten Fall zu Zahlungsausfällen führen.

➤ Fehlende Schulungen: Immer häufiger werden Angriffe durch Innentäter ausgelöst. Die Gründe für solche Angriffe sind vielschichtig, wie Dirk Bingler, Sprecher der Geschäftsführung bei GUS Deutschland berichtet: „Sie reichen von Enttäuschung, Frust am Arbeitsplatz und privaten Problemen bis hin zur einfachen Unkenntnis über sensible Schwachstellen in Arbeitsabläufen." Das fehlende Bewusstsein für potenzielle Gefahren ist groß, reicht doch ein unbedachter Klick auf E-Mail-Anhänge aus, um schädlicher Software Zugang zu gewähren.

Mehr Sicherheit für ERP-Systeme

Risiko erkannt, Gefahr gebannt? So einfach ist es leider nicht. Auch wenn die oben aufgeführte Liste schon erste Handlungsfelder aufzeigt, muss jedem IT-Verantwortlichen, aber auch Unternehmensentscheider bewusst sein: Den einen ultimativen Sicherheitstipp gibt es nicht. Es ist vielmehr die Kombination aus mehreren Maßnahmen. Um diese zu bestimmen, helfen die Punkte der Guideline (siehe oben).

ERP-Sicherheit bedeutet IT-Sicherheit

Veraltete Software stellt ein nicht zu unterschätzendes Risiko dar. Ob primäre oder sekundäre Schäden: Jedes Unternehmen muss die ERP-Schwachstellen ernst nehmen und zügig handeln. Verglichen mit den möglichen Verlusten lohnt jedes Investment in die Sicherheit der IT-Infrastruktur. Wer hier spart, handelt leichtsinnig. Was es braucht, ist neben dem Wissen um die Schwachstellen und Tipps zur Lösung die feste Verankerung der ERP-Security in einem durchdachten Sicherheitskonzept.

Matthias Weber, Inhaber des Beratungsunternehmens Mwbsc

WIE SCHÄTZEN SIE DEN DIGITALEN REIFEGRAD IN IHREM UNTERNEHMEN DERZEIT EIN?

BERND GREIFENEDER,

Gründer und CTO von Dynatrace, Anbieter von APM-Lösungen (Application Performance Management)

Drews: Wir sehen interne digitale Prozesse als Voraussetzung, um unsere Kunden durch vollständige digitale Einbindung unserer Systeme bei der Optimierung ihrer Wertschöpfungsprozesse zu unterstützen. Überall, wo es sinnvoll ist, setzen wir digital abgebildete Prozesse in der internen Bearbeitung von Projekten für mehr Effizienz und Transparenz ein. Bei Neu- und Weiterentwicklungen sind Sensorik und Aktorik sowie digitale Kommunikation wichtig – immer in Verbindung mit softwareseitiger Datenverarbeitung. Wir sind also mit unseren Anlagen mitten drin in der Digitalisierung. Aber auch wir stehen immer wieder vor Herausforderungen.

Greifeneder: Als ein marktführendes Unternehmen ist es positiv zu wissen, dass es noch viel Potenzial in der eigenen Digitalisierung gibt. Das bedeutet weitere Chancen, um den Vorsprung zur Konkurrenz noch mehr auszubauen. Speziell in unserem raschen Wachstum am Weltmarkt bedeutet Digitalisierung innovative Services und Self-Services anzubieten, um die Kundenzufriedenheit konstant hoch zu halten. Nur so ist ein überproportionales Wachstum von Kunden versus Mitarbeitern umsetzbar. Und es gilt auch, sich damit von der Konkurrenz noch weiter zu differenzieren. Die Customer Experience darf sich nicht nur auf das auf künstlicher Intelligenz aufgebaute Produkt beziehen, es muss sich auf alle Touchpoints des Unternehmens beziehen.

Middelhauve: Wir arbeiten ständig an der Erweiterung der digitalen Infrastruktur der Universität Bonn – einen Hochschullehrer, der nicht über Facebook und Co. erreichbar ist, gibt es bei uns nicht mehr. Dennoch ist die Digitalisierung nicht so weit fortgeschritten, wie wir das gerne hätten. Aber die Studierenden können auf fachbezogene E-Learning-Plattformen zugreifen, die die Kommunikationsplattform zwischen ihnen und den Hochschullehrern bilden. Zudem sind sie in der Lage, über die universitätsweit implementierte E-Campus-Plattform Informationen zu Lehrveranstaltungen abzurufen und Dokumente herunterzuladen. Unsere Verwaltungsstrukturen sind jedoch noch stark von papiergestützten Workflows abhängig – auch aufgrund der Gesetzgebung. Dies wird sich voraussichtlich in 2018 mit der Einführung eines ERP-Systems ändern.

WAS UNTERNEHMEN SIE, DAMIT SICH IHRE MITARBEITER RASCH IN DIE DIGITALE ARBEITSWEISE EINFINDEN UND FÜR DIESE BEGEISTERN?

RALF DREWS,

Geschäftsführer der Greif-Velox Maschinenfabrik

Drews: Schon im Recruiting achten wir darauf, Mitarbeiter zu gewinnen, die unsere Werte teilen und bereit sowie begeisterungsfähig für die Arbeit in einem agilen Unternehmen sind. Um die Mitarbeiter optimal in unsere internen digitalen Prozesse einzuführen, bieten wir beim Onboarding Schulungen an. Insbesondere bei Tätigkeiten, die spezielle Softwarekenntnisse erfordern. Darüber hinaus konzentrieren wir uns darauf, die Vorteile, die die Digitalisierung der Arbeitswelt mit sich bringt, bestmöglich zu nutzen. Dies erfordert aber auch kontinuierliches Hinterfragen, um unsere Arbeit und die Prozessabwicklung zu verbessern. Bei all dem darf nicht vergessen werden, dass der Mitarbeiter im Mittelpunkt stehen sollte. Daher verfolgen wir den Weg, Ideen unserer Mitarbeiter agil und unkompliziert umzusetzen.