Setzen Sie nicht auf Graumarktlösungen

Als COO der OTRS Gruppe macht mich die Kompetenz unserer globalen Teams sehr stolz. Sie haben 735.000 Zeilen professionell entwickelten Code produziert, der **OTRS** speziell mit dem sich permanent ändernden geschäftlichen Umfeld und modernsten Sicherheitsstandards Schritt halten lässt. In den letzten zehn Jahren wurden von ihnen **Tausende von OTRS-Instanzen** in den unterschiedlichsten Branchen und Unternehmensbereichen implementiert. Als hoch qualifiziertes Expertenteam arbeiten sie unermüdlich daran, dass unsere Kunden den größtmöglichen Nutzen aus unseren Service-Management-Lösungen gewinnen können.

Die Zusammenarbeit mit Experten, die qualitativ hochwertige Lösungen liefern, schützt Ihr Unternehmen vor ungeplanten Kosten, gefährlichem Datenverlust, Sicherheitsproblemen und hilft Ihnen sogar, wenn Sie in schon veralteten Technologien feststecken.

Die folgenden Berichte erzählen Begebenheiten, die unser Team in Unternehmen (Firmennamen sind auf Anfrage erhältlich) erlebt hat, die zuvor mit Graumarktanbietern zusammengearbeitet haben: Sie haben bereits eine ähnliche Erfahrung gemacht oder evaluieren gerade? **Kontaktieren Sie die OTRS Gruppe, den offiziellen OTRS-Produkthersteller**, um Ihre Situation zu besprechen. Wir helfen Ihnen gerne weiter.

www.otrs.com
sales@otrs.com

INHALT

DIE KOSTEN VON DATENVERLUST

– Francisco Cruz, GM OTRS Mexiko –

Anfängliche Einsparungen führen später häufig zu erheblichen Mehrkosten. Der Erfolg Ihres Geschäftes hängt u. a. von der Einhaltung von SLAs und zufriedenen Kunden ab. Eine verlorene Fallhistorie oder ausufernde Ticketzeiten können schwerwiegende finanzielle Folgen haben.

Wenn wir Systeme upgraden, ist die größte Sorge unserer Kunden fast immer, ob alle Daten weiterhin verfügbar sind. Insbesondere bei genauen SLAs wollen Kunden sicherstellen, dass sie zu jedem Zeitpunkt Zugriff auf die Ticketzeiten und -historie behalten.

Bei einer früheren Zusammenarbeit mit Graumarktanbietern ist die Aufbewahrung der Daten jedoch nicht immer möglich. Aus unserer Erfahrung passieren häufig diese zwei Dinge:

1. Graumarktanbieter haben nicht genügend Kenntnisse über **OTRS** selbst, so dass sie bestehende Features „neu erstellen“; das hat zur Folge, dass sie viele unnötige Änderungen und Modifikationen vornehmen. Das Feature mag dann zwar funktionsfähig sein, gleichzeitig haben sie aber das System im Prozess signifikant verändert.
2. Es entsteht in gewissem Sinne ein neues „Produkt“, weil Verzeichnisse und der Quellcode unsachgemäß modifiziert wurden.

Aufgrund von nicht systemkompatiblen Anpassungen durch den Graumarktanbieter hätte ein neuer Kunde bei der Migration 86% seiner Daten verloren. Das System kann nur noch archiviert werden und der Kunde bezahlt dafür, wieder bei Null zu beginnen.

Beides provoziert Probleme beim Upgrade. Das Migrationsskript führt routinemäßig eine Überprüfung der Verzeichnisse durch, um festzustellen, ob alles Benötigte vorhanden ist und ordnungsgemäß funktioniert.

Wenn sich das System im Originalzustand befindet, wissen unsere Entwickler, was sich von einer Version zur nächsten geändert hat und aktualisieren das Skript entsprechend. Damit wird sichergestellt, dass es diese Änderungen berücksichtigt und reibungslos durchläuft. ABER wenn die Verzeichnisse geändert wurden, schlägt das Skript vollständig fehl oder es löscht eben jene, die es in dieser Form nicht kennt.

Wenn ein solches Verzeichnis verloren geht, beispielsweise eines, welche sämtliche Kundendaten verwaltet, sind auch die darin befindlichen Informationen verloren. Und nicht nur das! Auch alle Funktionen und Prozesse, die auf diesem Verzeichnis basieren, arbeiten fehlerhaft, weil dieses nicht mehr als Referenz zur Verfügung steht. Können Sie sich vorstellen, was es bedeutet, den Zugriff auf alle Daten Ihrer Kunden zu verlieren?

Wir hatten Kontakt zu einem Unternehmen, das Workforce-Management-Lösungen anbot. Ihr System war so stark modifiziert worden, dass ein Upgrade nicht mehr möglich war. Sie steckten buchstäblich fest. An diesem Punkt gerät ein Unternehmen tatsächlich in erhebliche Schwierigkeiten. Denn einerseits ist ihr System anfällig, weil veraltet und ohne die neuesten Sicherheitspatches und damit nicht mehr nutzbar. Auf der anderen Seite muss es als Archiv erhalten werden. Gleichzeitig muss für eine neue Instanz bezahlt und weiter investiert werden, um diese entsprechend ihren Bedürfnissen anzupassen.

Was sich im ersten Schritt als Chance anbot, Geld zu sparen, vielleicht bei der Beratung, dem System selbst oder beim Support-Paket erweist sich später als echte Fehlentscheidung. **Denn am Ende geben sie oft doppelt so viel aus.**

VERLUST VON AGILITÄT: GRAU-MARKTANBIETER VERLANGSAMEN IHRE ANPASSUNGSFÄHIGKEIT

– Nils Leideck, Produktmanager bei OTRS –

Agilität wird durch flexible Tools und einfachen Datenzugriff ermöglicht. Die Zusammenarbeit mit Graumarktanbietern minimiert beides und lässt Unternehmen in der Vergangenheit verharren.

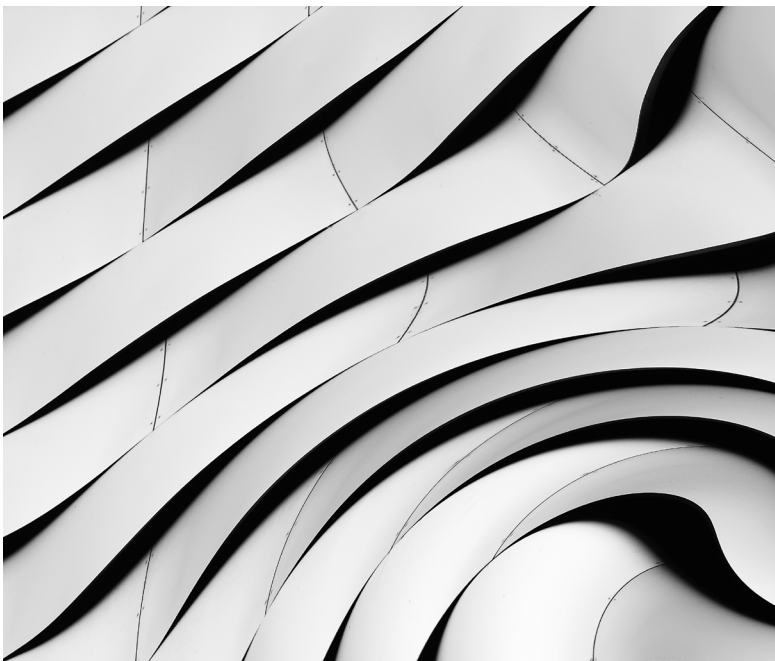
ag.il.i.ty (Substantiv)
die Fähigkeit, sich schnell und einfach zu bewegen.

Wie agil sind Sie, wenn Sie an einen Dienstleister oder veraltete Technologien gebunden sind?

Als Produktmanager ist es meine Aufgabe, sicherzustellen, dass unsere Teams agil arbeiten und es unseren Kunden ermöglicht wird, dasselbe zu tun. Agiles Arbeiten bedeutet, dass Sie beispielsweise die Arbeitsweise Ihres Service Desk, Ihrer Vertriebsabteilung oder Ihrer DevOps-Teams unabhängig von eingesetzten Tools jederzeit ändern können. So können Sie Mitarbeiter flexibel versetzen, aber die Prozesse und Tools unverändert lassen. Oder Sie können das Tool wechseln, aber die Mitarbeiter an Ort und Stelle belassen.

Graumarktanbieter machen das schwierig.

Wenn Ihr System stark individualisiert wurde, müssen Sie an den Graumarktanbieter herantreten, um all diese Individualanpassungen zu bearbeiten. Am Ende entsteht dadurch ein eigenes Projekt, das mit zusätzlichen Kosten und langen Fristen verbunden ist. Selbst für ein schnelles Update können Sie nicht einfach einen Termin anfordern und dann ist es erledigt. Sie müssen ein Projekt mit dem Graumarktanbieter aufsetzen.



Jetzt reden wir von der typischen Wasserfallmethode. Allein die Art der Zusammenarbeit mit einem Graumarktanbieter schränkt die Möglichkeiten eines Unternehmens ein, wirklich agil zu arbeiten.

Kürzlich habe ich mit einem Kunden zusammengearbeitet, der bestimmte Module von einem Graumarktanbieter gekauft hat. Die Module wurden als „OTRS-verifiziert“ bezeichnet, waren es aber keineswegs.

Tatsächlich haben sie einige der Sicherheitseinstellungen deaktiviert.

Darüber hinaus hatte der Anbieter die Datenbank so modifiziert, dass ein Login erforderlich war, so dass der Kunde, selbst wenn er es wollte, das System nicht aktualisieren oder einfach zu einem anderen Anbieter wechseln konnte.

So etwas kommt nicht selten vor, und es hindert Unternehmen daran, sich für andere Anbieter zu entscheiden, was ebenfalls die Agilität einschränkt. Wenn Sie Ihr Business aus irgendeinem Grund anpassen wollen – bedingt durch Standort-, oder neue regulatorische Anforderungen oder einfach nur aufgrund anderer Servicebedürfnisse — sind Sie gezwungen, das System aufzugeben und bei einem anderen Anbieter neu anzufangen.... das entspricht nicht dem Verständnis eines modernen agilen Denkansatzes.

Ich sehe, dass dies mehr und mehr zu einem Problem wird. Da künstliche Intelligenz, Analytik und Business Intelligence immer mehr an Bedeutung gewinnen, müssen Unternehmen sicherstellen, dass ihre Daten so strukturiert sind, dass sie die Vorteile moderner Tools und Prozesse optimal für sich nutzen können. Das bedeutet, dass Sie auch Updates noch schneller nutzen können müssen. Mit einem Graumarktanbieter werden Sie dazu kaum in der Lage sein.

ERHALTEN SIE DAS, WOFÜR SIE BEZAHLT HABEN?

– John Coggins, Business Relationship Manager –

Was tun Sie, wenn Sie statt dem, was Ihnen beim Kauf versprochen wurde, etwas ganz anderes bekommen haben? Wir berichten über einen Fall, bei dem der Benutzer noch einmal von vorne beginnen musste.

Ich bin seit über sechs Jahren bei der OTRS Gruppe in verschiedenen Funktionen für unser Support-Team tätig. Im Laufe dieser Jahre habe ich alle möglichen Probleme kennengelernt, die Kunden durch die Zusammenarbeit mit Graumarktanbietern in eine schwierige Lage gebracht haben. Manchmal wird die Verzeichnisstruktur und die Datenbank geändert, so dass Verzeichnisse nicht mehr in das OTRS-Schema passen. Diese Kunden können während des Upgrades keine wichtigen Sicherheitsupdates oder den Zugriff auf neue Funktionen erhalten.

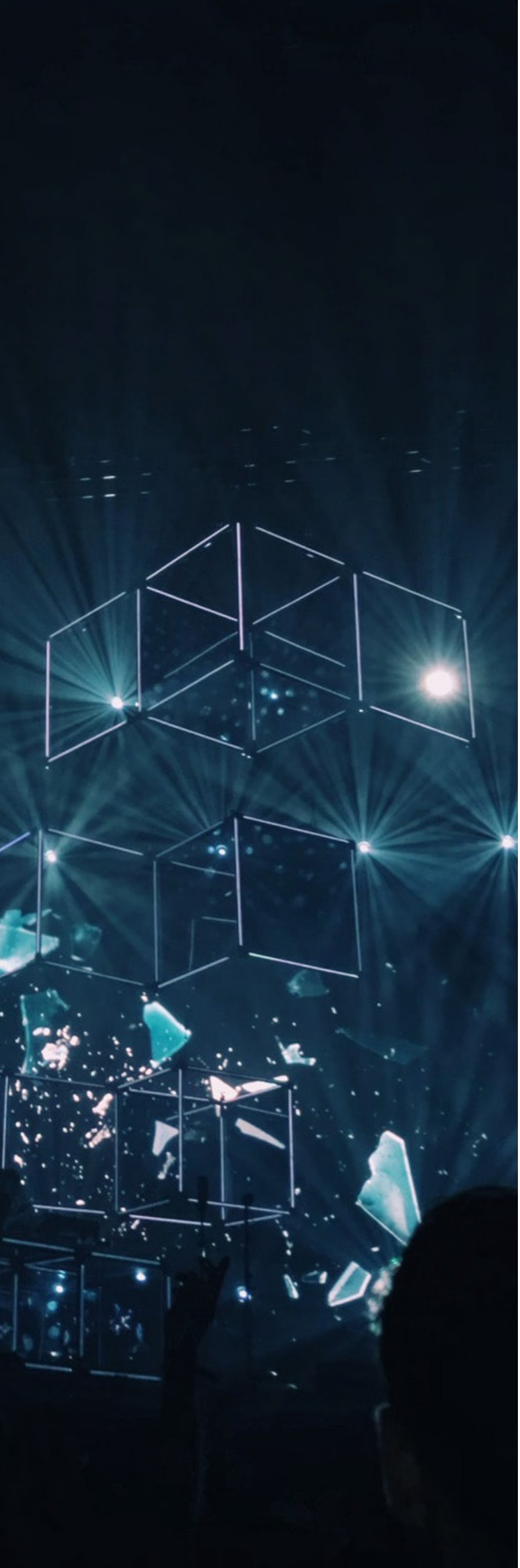
Manchmal bieten Graumarktanbieter an, die ((OTRS)) Community Edition auf die neueste Version zu einem reduzierten Preis upzudaten, scheitern dabei und können nicht weitermachen. Die Benutzer haben keinen direkten Support und können das System nicht wiederherstellen. Können Sie sich vorstellen, die komplette Dokumentation, alle Reports und implementierte Automatisierung zu verlieren, die sich Ihr Unternehmen aufgebaut hat?

Im Jahr 2017 legte NotPetya weltweit Großunternehmen lahm, indem eine bekannte Sicherheitslücke auf nicht gepatchten Computern genutzt wurde. Dadurch wurde der Betrieb der fünftgrößten Reederei der Welt buchstäblich eingestellt. Die geschätzten Gesamtkosten lagen bei über USD 10 Milliarden.

Im Moment arbeite ich mit einem Kunden zusammen, der sich an die OTRS Gruppe gewandt hat, weil er Schwierigkeiten hatte, seinen Dienstleister dazu zu bringen, wesentliche Supportfragen zu beantworten. Der Kunde hatte keinen Zugriff auf die Admin-Tools; grundlegende Aufgaben, wie das Zurücksetzen des Passworts, sollten beim Graumarktanbieter bis zu 14 Tage in Anspruch nehmen. Andere Anfragen benötigten sogar 21 Tage und es gab Situationen, in denen der Anbieter einfach gar keinen Support leisten konnte.

Also wandten sie sich an die OTRS Gruppe als Produkthersteller, um zu sehen, welche Lösungen wir anbieten können. Beim Betrachten ihres Systems stellten wir schnell fest, dass das, was der Kunde für **OTRS 7** hielt, tatsächlich **OTRS 6.0.3** war. Der Graumarktanbieter hatte die Release-Dateien gefälscht. Er hatte einen Skin erstellt, der **OTRS 7** nachahmt, aber das eigentliche System war nicht das, wofür der Kunde bezahlt hatte: Es wurde deutlich reduziert und viele Funktionen und Funktionalitäten von **OTRS 7** fehlten.

Dies brachte den Kunden in eine schwierige Situation. Er hat das System intern als Lösung vorgeschlagen und verfügt jetzt nicht über die Funktionalitäten, die notwendig wären. Sie benötigen eine Service-Management-Lösung, aber was sie haben, kann nicht aktualisiert werden. Sie stehen vor einem völligen Neuanfang, ohne auch nur einen Teil der vorhandenen Daten, die mit dem gefälschten **OTRS 7** generiert wurden, überhaupt behalten zu können.



VERSTOSS GEGEN DIE DATENSCHUTZ-BESTIMMUNGEN

– Matheus Baeta, Geschäftsführer, OTRS Brasilien –

Zerstörte Architektur, nicht überprüfte Code-Änderungen, inkompatible Sicherheitsupdates.... Graumarktanbieter verfügen nicht über das notwendige Fachwissen, um Ihre Kundendaten sicher zu halten.

Beispiele für Datenregelungen	Wo	Mögliches Geldstrafe
DSGVO	Europa	EUR 20 Millionen oder 4% weltweiter Jahresumsatz
CCPA	Kalifornien USA	USD 7.500 pro Vergehen
LGPD	Brasilien	2% des Umsatzes in Brasilien bis zu BRL 50 Millionen
PDPA	Singapur	Bis zu SGD 1 Millionen

Die weltweiten Datenschutzbestimmungen sind für Unternehmen von zunehmender Bedeutung. Ausgelöst durch die Datenschutz Grundverordnung (DSGVO) hat man auf internationaler Ebene begonnen, sich genauer damit auseinanderzusetzen, wie Unternehmen mit Daten umgehen: Inzwischen werden Bußgelder verhängt, wenn Unternehmen Nachlässigkeit zeigen.

Nehmen wir zum Beispiel die jüngsten Fälle, in denen British Airways vom Information Commissioner‘s Office in der EU mit einer **Geldstrafe von 183 Millionen Pfund** belegt wurde, Equifax, mit der Federal Trade Commission und anderen in den USA **mit bis zu 700 Millionen Dollar** und Integrated Health Information Systems in Singapur mit einer **Geldstrafe von 700.000 Dollar.**

Es ist nur eine Frage der Zeit, bis die über 120 Länder, die über eine Datenschutzgesetzgebung verfügen, damit beginnen, diese strenger durchzusetzen. Schließlich ist das eine lukrative Einnahmequelle.

Veraltete Software ist eine große Schwachstelle für Unternehmen, wenn es um die Sicherheit ihrer Daten geht. Denken Sie nur an die WannaCry- und Petya-Angriffe im Jahr 2017. Dass dadurch mehr als 300.000 Systeme in 150 Ländern infiziert werden konnten, war eine direkte Folge der Verwendung veralteter Software.

Und das ist es, was bei Graumarktanbietern oft passiert. Kundensysteme veralten, weil die zusammengeschusterten Graumarkt-Systeme die zugrunde liegende OTRS-Architektur soweit zerstört haben, dass notwendige Updates nicht mehr möglich sind. Unternehmen und ihre Kundendaten sind Angriffen schutzlos ausgesetzt.

Manchmal sind Unternehmen auch durch nicht überprüfte Code-Änderungen gefährdet — sei es aufgrund unlauterer Absichten oder einfach wegen mangelnder Expertise. Aktuell arbeite ich gerade an einen solchen Fall. Als wir das System eines Kunden überprüften, entdeckten wir eine beträchtliche Anzahl von Code-Änderungen, die dieses System dauerhaft und mit klarer Absicht an eine ältere Legacy-Version gebunden haben, ohne Sicherheitsupdates seit 2017.

Warum ist das wichtig? Seit 2017 gab es 15 Sicherheitslücken, für die Patches in **OTRS** veröffentlicht wurden.

Unternehmen, die Patches nicht ordnungsgemäß installieren, sind in Gefahr: Tatsächlich sind mehr als die Hälfte aller gemeldeten Datenschutzverletzungen auf nicht gepatchte Schwachstellen zurückzuführen, von denen einige ein Unternehmen lahmlegen können. So greift Borontok in jüngster Zeit Linux-Systeme (einschließlich Dateien, Registrierung, Programme und Einstellungen) an und zwingt Unternehmen, 75.000 US-Dollar (in Bitcoin) zu zahlen oder ihre Dateien innerhalb von drei Tagen löschen zu lassen. Cayosin ist ein Beispiel für ein sich entwickelndes Botnetz, das mehrere Schwachstellen ausnutzt, was am häufigsten zu Distributed Denial of Service (DDoS)-Angriffen führt. Unternehmen, die die richtigen Patches angewendet haben, sind sicherer; diejenigen, welche das nicht getan haben, sind den Risiken voll ausgesetzt.

Ein Kollege meines Teams arbeitet mit einem anderen Unternehmen zusammen. Die Untersuchung dieses Systems ergab, dass eine beträchtliche Anzahl von Webservices ausgeführt und kontinuierlich Daten an die ungesicherten Server des Graumarktanbieters übertragen wurden. Der Kunde hatte keine Ahnung, jedoch ist natürlich der Kunde letztendlich für die Daten verantwortlich.

Wenn Sie keine offiziellen Lösungen verwenden, wissen **Sie einfach nicht, ob jemand Zugriff auf Ihre Kundendaten erhält, was er definitiv nicht haben sollte.** Dadurch sind die Unternehmen gefährdet für mögliche behördliche Bußgelder.

KOSTEN UND NUTZEN SIND NICHT DASSELBE

– Udo Kampelmann, Geschäftsführer, OTRS Asia –

Ein niedriger Anfangspreis kann zu teuren Nacharbeiten und künftigen Ineffizienzen führen.

Die meisten Führungskräfte, mit denen ich zusammenarbeite, sind stringent ergebnisorientiert, wenn es um ihre Projekte geht. Sie wollen die aktuelle Technologie zu einem möglichst niedrigen Preis und die Anbieter von Graumärkten sind schnell bereit, eine Programmierung billig anzubieten. Graumarktanbieter setzen ein Geschäftsmodell ein, das darauf ausgerichtet ist, schnelles Geld zu verdienen, anstatt auf langfristige Zuverlässigkeit, Vertrauenswürdigkeit und Geschäftsbeziehungen zu setzen.

Sobald Unternehmen den Graumarkt betreten, werden sie davon abhängig. Sie sind auf zusammengestückelte Software angewiesen, um ihr Geschäftsmodell am Laufen zu halten. Wenn Änderungen oder Modifikationen am Code erforderlich sind, wäre es aufwendig, einen Entwickler eingreifen zu lassen, die Logik dahinter zu verstehen und Anpassungen an die neuen Anforderungen des Kunden vorzunehmen. Wenn es ein Problem mit der Software gibt, dass sie unbrauchbar macht, könnte das Geschäft sogar zum Erliegen kommen.

Es ist verständlich, dass Unternehmen nach dem besten Preis suchen, aber dieser muss von unterschiedlichen Perspektiven betrachtet werden.

Die direkte Zusammenarbeit mit dem Produkthersteller zahlt sich in der Regel innerhalb eines Jahres aus. In nur 12 Monaten können Sie den nachhaltigen Wert für Ihre Kunden langfristig steigern.

Echte Disruptoren, die die Technologiebranche in die Zukunft führen — die die Vorteile von KI, Big Data und Cloud Optionen nutzen werden, um innovative Kundenerlebnisse zu schaffen — verstehen, dass es für ein Unternehmen notwendig ist, seine Ergebnisse kontinuierlich durch Digitalisierung zu verbessern.

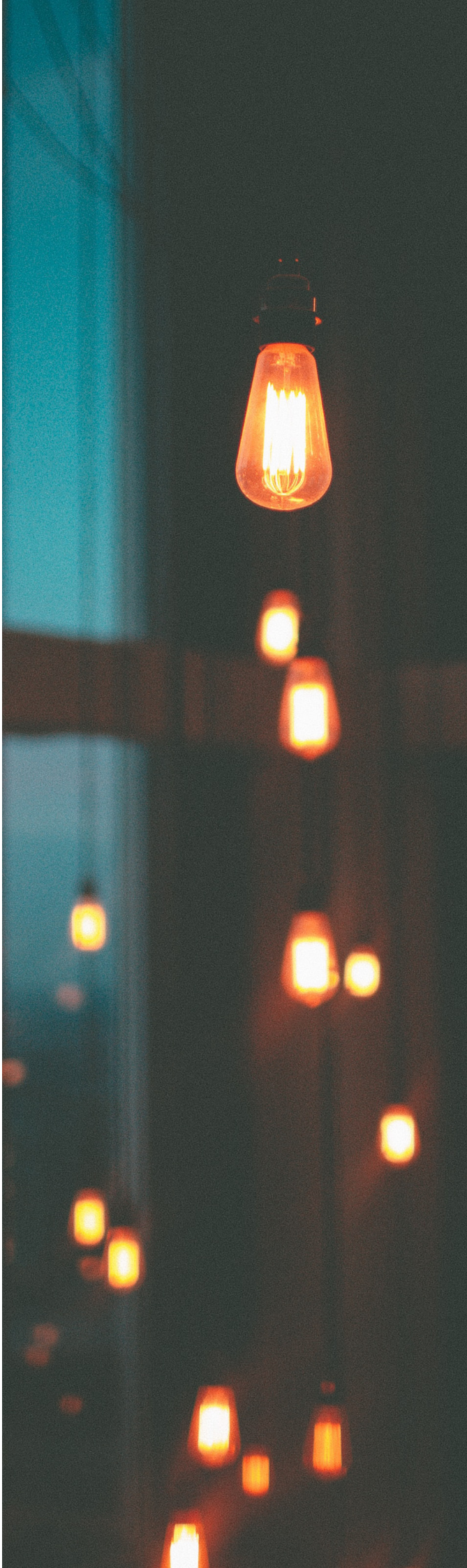
Sie wissen, dass sie sich auf die Verbesserung der Effizienz, stärkere Kundenbindung, die Senkung der Kosten und Up-selling konzentrieren müssen, wenn sie die Nase vorn haben wollen. Wenn sie mit einem Graumarktanbieter zusammenarbeiten, hat das eine kontinuierliche und endlose Optimierung ihrer Technologielösungen zur Konsequenz, da der Graumarktanbieter immer nur einen unmittelbaren Bedarf deckt: Er entwickelt keine flexiblen langfristigen Lösungen. So wird das System, bei dessen Erwerb Sie heute ein wenig Geld gespart haben, langfristig laufende Investitionen erforderlich machen, um mit den sich im Laufe der Zeit ändernden Anforderungen Schritt zu halten.

Im Gegensatz zu Anbietern im Graumarkt verfolgen Produkthersteller einen weitaus ganzheitlicheren Entwicklungsansatz. Sie sind am Puls der Zeit und bewerten, welche Trends anhalten werden, um das Produkt langfristig zu verbessern und den Kunden Sicherheit zu geben. Sie wissen, wie man Anpassungsoptionen mit bereits bestehenden Funktionen kombiniert, um den größtmöglichen Nutzen für die Kunden zu erzielen. Ihrer finanziellen Sicherheit und Geschäftsstabilität kann man vertrauen. Sie haben Zugang zu und Einblicke aus der Zusammenarbeit mit Branchenführern, wie der Federal CERT Community in Deutschland.

Zumindest im Falle von **OTRS** werden Ihre langfristigen Geschäftsergebnisse Teil der Lösung. Dies gilt sogar, wenn Sie eine neue Funktion oder einen neuen Prozess benötigen: Jede Anpassung an Ihre Instanz erfolgt auf der Grundlage von Best Practices, **so dass sie nicht mit jedem neuen Update überarbeitet und bezahlt werden müssen**. Tatsächlich werden die Implementierungskosten oft sogar teilweise von der OTRS Gruppe getragen.

Das konkrete Ergebnis der Entscheidung für den Produkthersteller gegenüber einem Graumarktanbieter ist, dass Ihre Lösung viel einfacher auf zukünftige Prozessänderungen reagieren kann, die zur Effizienzsteigerung, Erhöhung der Kundenbindung und des Upselling notwendig sind. Und das langfristig zu einem vernünftigeren Preis.

Billiger ist nicht immer besser. Und es ist nicht immer die beste Option für Ihr Unternehmensergebnis.



DIE WAHRHEIT IST SCHWARZ-WEISS

Der Begriff „Graumarkt“ ergibt sich aus der Tatsache, dass Anbieter eine Lösung außerhalb regulärer Vertriebskanäle verkaufen. Die Anbieter arbeiten in einer Grauzone — oft am Rande der Legalität.

Wir sind nicht die Einzigen, die die negativen Konsequenzen aus der Arbeit mit Graumarkt-Systemen beobachten. Aber sowohl als offizieller Produkthersteller von **OTRS** als auch als Unternehmen, das häufig mit Kunden konfrontiert wird, die mit Folgen von Graumarktlösungen zu kämpfen haben, wollen wir dazu beitragen, dass Sie (und Ihre Kunden) sicher und finanziell solide bleiben — nicht nur heute, und langfristig.

Wenn wir Ihnen bei der Suche nach Service-Management-Lösungen für Ihr Unternehmen behilflich sein können, oder wenn wir Sie darin unterstützen können, eine eventuell im Graumarkt entwickelte OTRS-Instanz zu überprüfen, wenden Sie sich bitte an **sales@otrs.com**

Die Kontaktinformationen der Regionalbüros sind verfügbar unter https://corporate.otrs.com/de/unternehmen/standorte/.

Verwenden Sie die folgende Checkliste, wenn Sie sich für einen Technologieanbieter entscheiden.

Schritt 1. Fragen Sie nach Lizenzierung und Verteilung.
Lassen Sie sich erklären, wie der Anbieter Zugang zur Software erhält, welche Rechte er hat und wie sich dies auf Sie und Ihr Unternehmen auswirkt.

☐ In welcher Beziehung stehen Sie zum offiziellen Produkthersteller?

☐ Können Sie eine schriftliche Erklärung vorweisen, die Sie zum Weiterverkauf des Produkts berechtigt? Haben Sie das Recht, die neueste Version des Produkts zu verwenden?

☐ Welche Art von Supportvereinbarung haben Sie zusätzlich zu den Vertriebsrechten mit dem Produkthersteller?

☐ Welche Garantie bieten Sie an? Habe ich Anspruch auf Herstellergarantien?

Schritt 2. Überprüfen Sie die Sicherheitsmaßnahmen.
Stellen Sie sicher, dass alle notwendigen Schritte unternommen werden, um Ihre Geschäftsabläufe und Kundendaten zu schützen.

☐ Sind Ihre Rechenzentren nach ISO 27001 zertifiziert?

☐ Welche Maßnahmen gibt es, um den physischen Zugriff auf unsere Daten zu beschränken?

☐ Wie verschlüsseln Sie Daten?

☐ Woher wissen wir, welche Daten an Ihre Server übertragen werden?

☐ Welche Backup-Verfahren gibt es?

☐ Sind Ihre Prozesse DSGVO-konform (oder andere anwendbare Datenvorschriften)? Wenn unser Kunde die Löschung der Daten wünscht, welche Garantien haben wir, dass Sie diese durchführen werden?

☐ Was passiert mit meinen Daten im Falle einer Vertragskündigung?

☐ Auswirkungen habe ich im Falle einer Verstoßes?

☐ Welche Prozesse gibt es, um mein System auf dem neuesten Stand zu halten? Wann und wie werden Patches vorgenommen?

Schritt 3. Bewerten Sie Training und Fachwissen.
Stellen Sie fest, ob der Anbieter über ausreichende Fachkenntnisse in der Arbeit mit der Software verfügt und gewinnen Sie Einblick in seine Unterstützungsmethoden.

☐ Sind Sie in Bezug auf dieses Tool/Produkt/Lösung zertifiziert?

☐ Wie lange sind Sie schon im Geschäft?

☐ Können Sie Referenzen von Kunden vorweisen, die dieses System zuvor unter Ihrer Leitung upgegraded haben?

☐ An wie vielen Installationen/Upgrades/Projekten haben Sie speziell mit diesem Produkt gearbeitet?

☐ Was ist die komplizierteste Konfiguration, die Sie je durchgeführt haben?

☐ Fragen Sie nach einer Referenzimplementierung und befragen Sie diese Kunden möglichst ohne Einbeziehung Ihres Lieferanten.

Schritt 4. Stellen Sie Fragen zur Nachhaltigkeit des Unternehmens.
Überprüfen Sie noch einmal, ob dies ein Partner ist, der Sie auch dann unterstützen kann, wenn Ihr Unternehmen wächst. Bleiben Sie nicht mit ihrer maßgeschneiderten Lösung auf sich selbst angewiesen, ohne Möglichkeit Hilfe zu erhalten, falls der Anbieter sich vom Markt zurückzieht.

☐ Was sind Ihre langfristigen Unternehmensziele? Stehen Sie weiterhin zur Verfügung, wenn wir Hilfe brauchen?

☐ Welchen Zugang zu den Administrationstools habe ich?

☐ Welche SLAs können wir erwarten? Wenn diese nicht erfüllt werden, welche Regressansprüche haben wir dann?

☐ Wenn unsere Geschäftsbeziehung enden sollte, welche Probleme würde ich haben, wenn ich einen neuen Berater / ein neues Support-Team suche?

☐ Auf welche Probleme stoße ich, wenn ich andere Tools integrieren möchte?