Ransomware – Schichtweise Verteidigung

Unternehmen benötigen Backup-Software, die nicht nur erstklassiges Backup und Recovery ermöglicht, sondern auch die Zugriffspunkte für Ransomware verringert.

Ransomware ist keine neue Erfindung. Sie ist schon seit langem im Umlauf, und solange Ransomware-Angreifer die Möglichkeit eines finanziellen Vorteils sehen, wird sie auch nicht verschwinden.

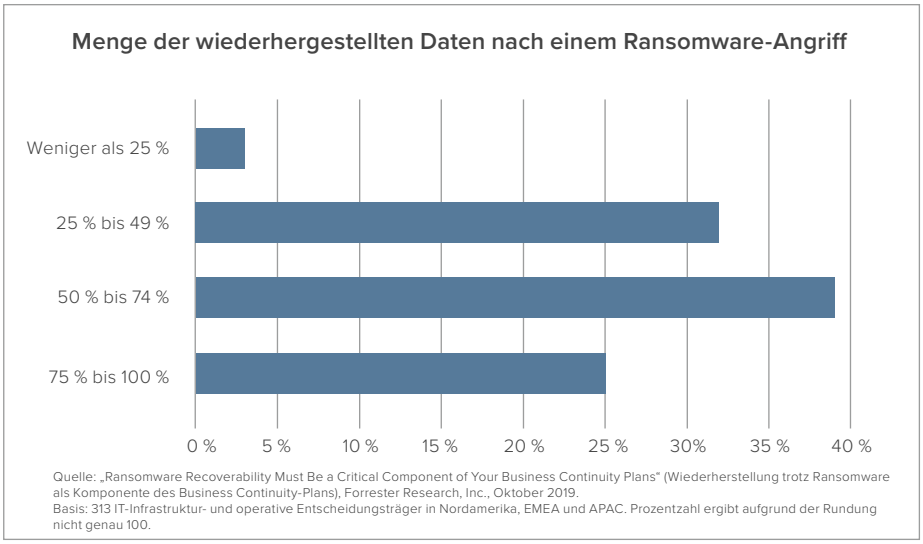
Laut einem Bericht von Forrester Research[1] aus dem Jahr 2019 ist die Anzahl der Ransomware-Angriffe im vorigen Jahr um über 500 % gestiegen. Außerdem schätzt Forrester, dass diese Angriffe die Unternehmen 11,5 Milliarden Dollar kosten – und dabei sind noch nicht einmal die immateriellen Kosten durch den Vertrauensverlust bei Kunden und Partnern eingerechnet.

Dazu kommen die Kosten, wenn nicht alle Daten nach einem Ransomware-Angriff wiederhergestellt werden können. Tatsächlich zeigte 2019 eine Umfrage von Forrester[2], dass nach einem Ransomware-Angriff nur 25 % der Umfrageteilnehmer angaben, dass sie zwischen 75 % und 100 % ihrer Daten wiederherstellen konnten. Dagegen gaben 39 % der Umfrageteilnehmer an, dass sie nur in der Lage waren, zwischen 50 % und 74 % ihrer Daten wiederherzustellen.

Da die Bedrohungslage und die Kosten durch Ransomware unverändert hoch sind, besteht die Herausforderung für IT und Backup-Admins darin, die Verteidigungs-schichten neu zu bewerten, die zur Abwendung der Ransomware-Risiken erforderlich sind.

> Ransomware-Angriffe sind um 500 % gestiegen und werden Unternehmen 11,5 Milliarden Dollar kosten.

[1] „Forrester's Guide to Paying Ransomware" (Anleitung zur Lösegeldzahlung bei Ransomware), Forrester Research, Inc., 5. Juni 2019
[2] „Ransomware Recoverability Must Be a Critical Component of Your Business Continuity Plans" (Wiederherstellung trotz Ransomware als Komponente des Business Continuity-Plans), Forrester Research, Inc., Oktober 2019.



Quelle: „Ransomware Recoverability Must Be a Critical Component of Your Business Continuity Plans" (Wiederherstellung trotz Ransomware als Komponente des Business Continuity-Plans), Forrester Research, Inc., Oktober 2019.
Basis: 313 IT-Infrastruktur- und operative Entscheidungsträger in Nordamerika, EMEA und APAC. Prozentzahl ergibt aufgrund der Rundung nicht genau 100.

Eine Umfrage von Forrester zeigte 2019, dass nur 25 % der Umfrageteilnehmer angaben, dass sie zwischen 75 % und 100 % ihrer Daten nach einem Ransomware-Angriff wiederherstellen konnten.

Allein drei Arten von Ransomware verursachten Schäden in Höhe von 1 Milliarde Dollar in mehr als 65 Ländern.

RANSOMWARE NUTZT VERSCHIEDENE METHODEN FÜR DEN ZUGRIFF

Es gibt verschiedene Methoden, die Ransomware nutzt, um sich Zugriff zu verschaffen. Einige könnten als „Sprühnebel-Angriffe" eingestuft werden, mit dem Ziel, so viele Opfer wie möglich zu erreichen. In letzter Zeit wurden jedoch häufiger bestimmte Unternehmenstypen angegriffen. Lassen Sie uns einige der bekannteren Beispiele untersuchen.

WannaCry

Diese Ransomware ist berühmt-berüchtigt und traf mit ihrem Angriff viele Unternehmen rund um den Globus. WannaCry nutzte eine bekannte Schwachstelle – Eternal Blue – und griff über diese Schwachstelle ältere und ungepatchte Systeme an, um in die IT-Umgebung zu gelangen.

Für den Angriff wurde die Sprühnebel-Methode verwendet: Massen-E-Mails mit Anhängen oder Links auf Websites, Dokumentverknüpfungen mit Dateifreigabe-Sites usw. Die meisten Instanzen erlangten Zugriff, wenn ein Endbenutzer ein Dokument oder ein Datenelement herunterlud, das dann auf der Hardware des Endbenutzers ausgeführt wurde.

Anschließend verschlüsselte die Ransomware die Daten, und die Hacker verlangten eine Lösegeldzahlung in Kryptowährung, um die Daten zu entschlüsseln. Dabei gab es natürlich keine Garantie, dass die Daten wirklich entschlüsselt würden, selbst wenn das Unternehmen das Lösegeld zahlte.

NotPetya

Im Gegensatz zu WannaCry ging es bei NotPetya nicht um ein Lösegeld, sondern um reine Zerstörung und um Chaos anzurichten. Die schnelle Verbreitung war hier die Strategie. Auch diese Ransomware baute darauf auf, dass jemand die Tools in das Unternehmen schleuste, bevor sie zuschlagen konnten. Hier wurde eine abgeänderte Version von Eternal Blue und eine übersehene Eternal Romance SMB-Schwachstelle genutzt.

BadRabbit

Laut WIRED-Magazin verbreitete sich BadRabbit über „Drive-by-Angriffe" auf regulären Websites. Wenn Endbenutzer eine normale Website besuchten, gab der Angreifer Malware getarnt als Adobe Flash-Installationsprogramm mit. Diese Malware sperrte dann sofort die infizierte Hardware. Es folgte eine Lösegeldforderung, in der Regel 280 Dollar in Bitcoins.

Allein diese drei Arten von Ransomware verursachten Schäden in Höhe von 1 Milliarde US-Dollar in mehr als 65 Ländern!

Quest

DIE NÄCHSTE PHASE

Ransomware hat eine neue Phase erreicht – mit einer gezielteren, wohlüberlegten Vorgehensweise. Einige Toolsets werden bereits als Ransomware-as-a-Service (RaaS) betrachtet. Diese offenen Durchlässe und kompromittierte Anmeldedaten werden an Kriminelle verkauft, die nichts als Lösegeld erpressen wollen.

Selbst die Finanzmodelle haben sich geändert. Vorbei sind die Zeiten, in denen Hacker Bitcoins im Wert von 300 Dollar wollten, um die Daten zu entschlüsseln. Heutzutage liegen die Lösegeldforderungen zwischen 1 und 10 Millionen Dollar. Zusätzlich nutzen die Angreifer neue Taktiken, um Lösegeld einzufordern, wie das Veröffentlichen der Unternehmensdaten, wenn kein Lösegeld gezahlt wird.

Dies stellt häufig an sich eine Datenschutzverletzung dar, sodass sich das Unternehmen aufgrund von Compliance-Verstößen bei Behörden wie GDPR, CCPA oder unter der neuen Gesetzgebung im Staat Washington HB1071 verantworten muss, was personenbezogene Daten und Sicherheitsverletzungen betrifft.

Die Angriffe ändern sich ebenfalls. Ein zunehmender Trend sind menschliche Aktivitäten zur Verlängerung der Angriffe. Lassen Sie uns einen Blick auf ein mögliches Ransomware-Szenario werfen.

BEISPIEL-SZENARIO

In diesem Abschnitt erkunden wir GPO-Angriffe mittels Gruppenrichtlinienobjekten. Gruppenrichtlinien gehören zur Kerninfrastruktur von Microsoft, um Benutzer und Computer in einer Windows-Unternehmensstruktur zu verwalten.

Microsoft beschreibt dies so: „Gruppenrichtlinieneinstellungen sind in einem GPO enthalten. Ein GPO kann die Richtlinieneinstellungen im Dateisystem und in Active Directory darstellen. Die GPO-Einstellungen werden von den Clients anhand der hierarchischen Struktur von Active Directory ausgewertet."

Sie haben wahrscheinlich schon die Bedeutung von Dateisystemen und Active Directory bemerkt. Ein erfolgreicher Angriff auf Ihr Active Directory ist so, als würden Sie die Hausschlüssel Ihrem schlimmsten Feind übergeben.

Diese Angriffe werden manchmal als Gruppenrichtlinien-Hijacking bezeichnet, die bekannte Schwachstellen nutzen, um die Kontrolle über das gesamte Unternehmen zu erlangen. Diese Art von Angriff hat den zusätzlichen Effekt, dass sie durch menschliche Aktivitäten verstärkt wird, um Dinge ständig zu verändern und einen Zugriffspunkt im angegriffenen Unternehmen offen zu halten.

SCHICHTWEISE VERTEIDIGUNG

Um die Bedrohungen durch Ransomware zu minimieren, müssen Unternehmen eine schichtweise Verteidigung aufbauen. Die hier angegebene Liste ist zwar nicht allumfassend und bietet keine Garantie gegen Ransomware-Angriffe, aber sie ist ein guter Einstieg, was beachtet werden muss und wie sinnvoll die bereits vorhandenen Maßnahmen sind.

Schulungen für Endbenutzer

Es ist unerlässlich, die Benutzer zu informieren und zu schulen und über die Risiken aufzuklären. Klären Sie sie darüber auf, wie Ransomware in ein Unternehmen gelangt (durch Downloads, Dateien, falsche Websites, Dateifreigabe-Sites, Phishing-Angriffe zum Abfassen von Benutzerdetails und Anmeldedaten).

Die Endbenutzer sollten außerdem auf physische Zugänge für Ransomware im Unternehmen achten. Es gibt Fälle, in denen infizierte USB-Sticks auf dem Parkplatz oder im Eingangsbereich herumlagen und dann von einem ahnungslosen Benutzer an ihren Laptop angeschlossen wurden.

Patching

Halten Sie Ihre Systeme immer auf dem neuesten Stand. Verlassen Sie sich nicht darauf, dass Sie schon daran denken werden oder sich an einen Zeitplan halten. Automatisieren Sie den Prozess mit einer vertrauenswürdigen Lösung wie Quest KACE Unified Endpoint Management. Überlassen Sie nichts dem Zufall. Führen Sie Patching für alle Computer, Clients und Server durch.

Nicht nur Windows

Gehen Sie nicht davon aus, dass es sich nur um eine „Windows-Sache" handelt. Linux ist ebenfalls Bedrohungen ausgesetzt, aktualisieren Sie also auch die Linux-Server regelmäßig.

Ein erfolgreicher Angriff auf Ihr Active Directory ist so, als würden Sie die Hausschlüssel Ihrem schlimmsten Feind übergeben.

Eine schichtweise Verteidigung ist die einzig wirksame Vorgehensweise. Sich nur auf Datensicherungslösungen zu verlassen, reicht als Vorbeugungsmaßnahme nicht aus.

Netzwerk-Monitoring

Stellen Sie sicher, dass Sie alles überwachen, was nach abgefangenem Datenverkehr aussieht. Routing-Änderungen, Scherz-Apps und Datenverkehrsumleitung sind Ausgangspunkte für den Zugriff auf die Unternehmensinfrastruktur durch „Man in the Middle“ (MITM)-Angriffe.

Datensicherung

Daten-Backups gehören ganz selbstverständlich dazu, oder? Ja, aber trotzdem befinden sich diese noch auf Servern und werden mit Betriebssystemen ausgeführt, was sie wiederum angreifbar macht. Außerdem haben Backup-Produkte, die Netzwerkfreigaben zum Speichern der gesicherten Daten verwenden, ein höheres Risiko, da die Netzwerkfreigaben ein beliebtes Ziel für Ransomware sind.

DATENSICHERUNG HAT AUCH GRENZEN

Alles in allem ist eine schichtweise Verteidigung die einzig wirksame Vorgehensweise. Sich nur auf Datensicherungslösungen zu verlassen, reicht als Vorbeugungsmaßnahme nicht aus.

Datensicherung ist eine reaktive Technologie. Sie reagiert auf eine Situation, die es erfordert, dass Daten wiederhergestellt werden. Eine Datensicherung sollte regelmäßig durchgeführt werden, um Datenverluste zu vermeiden. Sie kann jedoch nur effektiv wirken, wenn die Lösung außerdem Methoden umfasst, um den Verlust von Backup-Daten zu verhindern.

Nehmen Sie beispielsweise eine Situation, in der die Backup-Lösung eine Netzwerkfreigabe nutzt. Diese Freigabe ist zwar durch Benutzerkonten und Berechtigungen geschützt, aber trotzdem befindet sie sich im Netzwerk. Ein GPO-Angriff, der erweiterten Domänenzugriff auf Server und Clientrechner ermöglicht, mach es den Ransomware-Angreifern einfach, eine Netzwerkfreigabe zu verschlüsseln, die Backup-Daten enthält.

Datensicherungslösungen sind in den meisten Fällen ein Sicherheitsnetz. Doch mit der steigenden Anzahl von Ransomware-Angriffen wird deren Rolle im Unternehmen in Bezug auf die schnelle Wiederherstellung nach einem Ransomware-Angriff kritisch gesehen.

Um dies effektiv umzusetzen, muss die Backup-Lösung so widerstandsfähig wie möglich sein, ohne ihre Zweckmäßigkeit zu beeinträchtigen.

Bedenken Sie für einen Moment, was eine Backup-Lösung können muss: Sie muss alle Daten von A nach B verschieben, und zwar so schnell wie möglich. Das ist jedenfalls das, wonach die meisten Anwender suchen. Dies erfordert den Zugriff auf alle wichtigen Daten des Unternehmens, auf Anwendungen, Netzwerke, Produktionsspeicher usw. Genau genommen erhält die Lösung mehr Zugriff als die meisten Benutzer im Unternehmen, abgesehen vom Domänenadministrator.

Und doch gibt es noch immer Datensicherungslösungen, die nur unzureichend mit Standard-Benutzernamen und -Passwörtern geschützt sind. Oder die Datensicherungslösungen nutzen offene Freigaben, die genau das sind: weit offen. Wir haben es doch alle schon getan. Wir haben Berechtigungen für „Jeder“ freigegeben, damit etwas schnell funktioniert – doch dies ist auch der einfachste Zugriffspunkt für Ransomware.

SO KANN QUEST IHNEN HELFEN

Um die Risiken durch Ransomware effektiv zu minimieren, benötigen Unternehmen eine Datensicherungslösung, die zusätzliche Widerstandskraft beim Kampf gegen die Auswirkungen von Ransomware auf Backup-Lösungen bietet. Quest NetVault Plus bietet genau das.

NetVault Plus ist eine umfassende Datensicherungslösung für Unternehmen, die für modernste Rechenzentrumsanwendungen und deren Infrastruktur sowie für Cloud-Lösungen optimiert ist. Sie weist vielfältige Funktionalität auf, nicht nur beim Schutz sondern auch bei der Bereitstellung in der Serverarchitektur. NetVault Plus umfasst eine integrierte Software-definierte Speicherlösung für Deduplizierung, Komprimierung, Verschlüsselung, Replikation und Cloud-Integration.

Entdecken Sie, wie NetVault Plus Daten speichert. Es verwendet eine integrierte Speichertechnologie namens QoreStor. Diese Software-definierte sekundäre Speicherlösung ist speziell für Backup-Lösungen konzipiert. NetVault ist eng mit QoreStor integriert und nutzt das Protokoll Rapid Data Access (RDA).

Im Gegensatz zu Server Message Block (SMB), das für Windows-Freigaben verwendet wird, ist RDA kein offenes Protokoll. Es kann nicht direkt über ein Betriebssystem aufgerufen werden und erfordert eine Authentifizierung, die außerhalb des lokalen Servers bzw. des domänengesteuerten Konstrukts erfolgt. Bei Verwendung von NetVault Plus werden die Backup-Daten direkt von der Quelle zum Ziel geleitet, in diesem Falle QoreStor. Es sind keine herkömmlichen Medienserver erforderlich. Dadurch wird einerseits die Komplexität und andererseits das Risiko reduziert, da weniger Kernkomponenten angegriffen werden können.

Zusätzlich verwendet NetVault Plus quellseitige Deduplizierung, um die Datenmenge zu reduzieren, die über das Netzwerk vom Clientrechner an den Speicher gesendet wird. Somit wird die Exposition gegenüber Datenerfassungstechnologien weiter beschränkt.

Darüber hinaus wendet NetVault Plus eine Secure Connect-Technologie an, welche die Datenübertragung und Steuerbefehle in einem sicheren TLS 2.0-Layer verpackt. Dies ist ein wichtiger Schritt zur Beschränkung des Zugriffs auf Ihre Backup-Daten durch Ransomware. Natürlich hat NetVault Plus selbst ebenfalls Zugriff auf die Backup-Daten, also muss auch das berücksichtigt werden.

NetVault Plus verwendet quellseitige Deduplizierung, um die Datenmenge zu reduzieren, die über das Netzwerk vom Clientrechner an den Speicher gesendet wird – und beschränkt so die Exposition gegenüber Datener-fassungstechnologien .

Operative Verbesserungen durch NetVault Plus.

Element	Inhalt	Hinweise
NetVault Plus-Daten auf QoreStor	WORM	NetVault schreibt Backups als Datenstrom auf QoreStor. Dieser Datenstrom kann durch NetVault nicht geändert werden. NetVault kann den gesamten Datenstrom (das Backup) von QoreStor entfernen, aber nicht Teile davon.
Zugriff auf QoreStor (Protokoll)	RDA	NetVault kann nur über das RDA-Protokoll auf QoreStor zugreifen. Dieses Protokoll gibt es in unterschiedlichen Versionen. NetVault verwendet Version 2.0, die das Schreiben, Lesen und die Replikation von Daten zulässt. Es sind keine Änderungen möglich. Vom RDA in QoreStor geschriebene Daten können nicht über CIFS/SMB, NFS oder andere Protokolle abgerufen werden.
Zugriff auf QoreStor (Authentifizierung)	Benutzername/ Passwort	Der Zugriff auf QoreStor findet immer über ein Benutzerkonto mit Passwort statt. Die Passwörter sind verschlüsselt (AES) und werden über Verschlüsselung ausgetauscht (AES). Der Zugriff auf QoreStor auf Verwaltungsebene bietet keinen Zugriff auf die Daten, nur auf die Konfigurationseinstellungen.
Datenzugriff	RDA	Daten, die unter Verwendung des RDA-Protokolls gespeichert wurden, können nur über den ursprünglichen (Backup-)Server abgerufen werden. Ein alternativer Backup-Server erhält ohne die korrekten Anmeldedaten und die eindeutige ID keinen Zugriff auf die Daten.
Zugriff auf QoreStor	SSH	Es ist möglich, über SSH auf QoreStor zuzugreifen, Sie erhalten jedoch keinen Zugriff auf die Daten, sondern nur auf ein Menü mit Konfigurationseinstellungen. Für den SSH-Zugriff ist eine Passwortanmeldung erforderlich.
Speichertyp	Deduplizierung	Alle Daten werden in QoreStor in einem eigenen Format gespeichert. Es gibt kein lesbares Dateisystem mit sichtbaren Dateien im Backup-Datenstrom, die für Dateien oder Teile davon stehen.
Verwendetes Betriebssystem	Linux	QoreStor läuft unter Linux und kann mit einer Minimalinstallation ausgeführt werden. Es unterstützt die Verwendung einer Linux-Firewall, deren Regeln während der Installation hinzugefügt werden. Außerdem wird die Verwendung von SELINUX unterstützt.
Patching	Betriebssystem	Es wird empfohlen, die Betriebssystem-Patches regelmäßig zu aktualisieren, um den Schutz des Betriebssystems gegen bekannte Schwachstellen sicherzustellen.
Protokoll	RDA	RDA ist ein eigenes Protokoll von Quest. Es gibt keine öffentliche Beschreibung dieses Protokolls. RDA wird ausschließlich in Produkten von Quest verwendet. Derzeit in NetVault und vRanger.

Quest

Sie haben vielleicht auch schon festgestellt, dass Ransomware bisher überwiegend Windows-basierte Systeme betraf – einerseits aufgrund der Beliebtheit des Systems, andererseits durch die Anzahl vorhandener Benutzerclients/-Endpunkte, die Ransomware-Angreifer nutzen können.

NetVault Plus minimiert diese Bedrohung, indem der Server und dessen Infrastrukturkomponenten unter Linux installiert werden. Auch wenn er damit nicht komplett unangreifbar ist, wird durch die Installation des Servers unter Linux die Anzahl potenzieller Bedrohungen reduziert. Da NetVault Plus eine komplett heterogene Lösung ist, deren Kernkomponenten unter Linux ausgeführt werden, schützt NetVault Plus Windows, Unix, Linux sowie Anwendungsdaten und Virtualisierungsplattformen auf die gleiche Weise.

Eine weitere Überlegung ist die Art der Zugriffserteilung. NetVault Plus verfügt über zwei Hauptmethoden der Zugriffserteilung: Integration in einen Verzeichnisdienst oder eigene rollenbasierte Zugriffsmechanismen. Angesichts der potenziellen Probleme mit GPO-Angriffen, die wir bereits erläutert haben, sollten wir berücksichtigen, dass eine solche Sicherheitslücke den Zugriff auf die Backup-Anwendung ermöglichen kann, wo es zu systematischen Datenlöschungen kommen könnte.

Doch NetVault Plus verfügt über eine robuste rollenbasierte Zugriffsmethode, ohne dass ein Dienst wie Active Directory integriert werden muss. Auch wenn dies etwas weniger komfortabel für die Festlegung von Benutzern und Gruppen ist, wird dadurch eine stärkere Trennung von der Produktionsumgebung erreicht und damit auch potenzielle Zugriffe durch unerwünschte Dritte verhindert.

FAZIT

Letztendlich können sich selbst die am besten vorbereiteten Unternehmen nicht vollständig gegen Ransomware-Angriffe schützen. Sie können jedoch die Risiken minimieren, indem Sie eine Backup-Lösung verwenden, mit der Sie nicht nur alle Ihre Daten schnell wiederherstellen können, sondern die außerdem:

- Risiken der Auswirkungen von Ransomware auf Ihr Unternehmen beseitigt
- Die Anzahl an angreifbaren Kernkomponenten reduziert
- Exposition gegenüber Datenerfassungstechnologien beschränkt
- Zugriff auf Backup-Daten für Ransomware beschränkt

Weitere Informationen zu NetVault Plus finden Sie unter: https://www.quest.com/de-de/products/netvault/netvaultplus.aspx

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Cloud-Erweiterung, Hybrid-Rechenzentren, Sicherheitsbedrohungen und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Wir sind der globale Anbieter für 130.000 Unternehmen in 100 Ländern, einschließlich 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 entwickeln wir eine Palette von Lösungen, die aktuell Datenbankverwaltung, Datensicherung, Identitäts- und Zugriffsverwaltung, Microsoft-Plattformverwaltung sowie die Verwaltung vereinheitlichter Endgeräte umfasst. Mit Quest investieren Unternehmen weniger Zeit in die IT-Administration und haben mehr Zeit für geschäftliche Innovationen. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:
www.quest.com/de-de/company/contact-us.aspx