NetIQ

Sicherer moderner Fernzugriff

Der Blick über den Tellerrand – oder über das Gebäude hinaus

Der Trend in Unternehmen, Mitarbeitern die Arbeit von außerhalb des Büros per Fernzugriff zu ermöglichen, hält nicht nur unvermindert an, sondern nimmt in bemerkenswertem Maße zu. Diese sogenannte Telearbeit ist nicht länger auf Außendienstmitarbeiter oder jene beschränkt, die gelegentlich ihre privaten Geräte für geschäftliche Aktivitäten außerhalb der Geschäftszeiten nutzen. Stattdessen ist die Telearbeit inzwischen zu einem festen Bestandteil der modernen Arbeitswelt geworden – egal an welchem Ort. Sie erstreckt sich mittlerweile auf alle Bereiche eines Unternehmens. Wenn die Sicherheitsvorkehrungen für den dazu benötigten Fernzugriff jedoch nicht auf den neusten Stand gebracht werden, kann Telearbeit potenziell zum finanziellen Risiko werden.

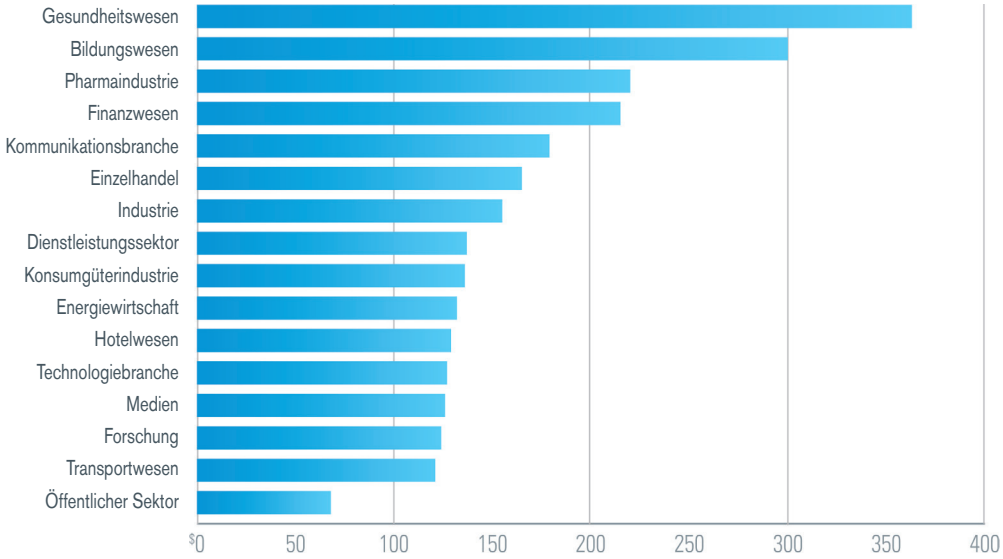
Hier stellt sich die Frage, wie weit sich dieser Trend noch fortsetzen wird und in welchem Umfang die IT-Abteilungen darauf reagieren müssen. In einer Umfrage[1] unter Beschäftigten im Personalwesen gab über ein Viertel der Befragten an, dass ihr Unternehmen zumindest ein paar Telearbeiter beschäftigt. In multinationalen Organisationen ist diese Zahl sogar mehr als doppelt so hoch, d. h. 2 von 3 der dortigen Mitarbeiter nutzen inzwischen Modelle für Telearbeit. Der Prozentsatz schwankt natürlich in den verschiedenen Branchen.

Flash Point-Paper
Einrichten effektiverer Zugriffskontrollen

Erfolgsentscheidende Faktoren für die Produktivitätssteigerung von Remote-Mitarbeitern:

- *Die richtige Kombination aus Menschen, Einrichtungen und Technologien*
- *Die richtige Kommunikationsausrüstung, Schulung und Unterstützung*
- *Konnektivitätstechnologien: Plug and Play, Datenfreigabe, Netzwerkzugriff, virtuelle Sitzungen und Drahtlosfunktionen*
- *Optimierte Nutzung von Online-Ressourcen*
- *Leistungsmessung*

Die Kosten für Datendiebstahl belaufen sich in den USA auf durchschnittlich 217 USD.



Quelle: 2015 Ponemon Breach Study

Die mit Telearbeit verbundenen Risiken

Fast scheint es, als würde jede Woche eine andere Organisation in die Schlagzeilen geraten, in denen der Verlust von Unternehmensdaten in großem Stil bekannt (oder zugegeben) wird. Die betroffenen Unternehmen sind häufig allgemein hoch angesehen und stammen aus praktisch allen Branchen.

In den letzten zehn Jahren hat das Ponemon Institute jährlich Umfragen zu den stetig steigenden Kosten durchgeführt, die durch diese Cyber-Angriffe verursacht werden. Tatsächlich sind die Gesamtkosten für Datendiebstahl in den vergangenen zwei Jahren um 23 Prozent gestiegen. Weltweit belaufen sich die Kosten pro entwendetem Datensatz inzwischen auf durchschnittlich 154 USD, von denen ein beachtlicher Teil durch den Verlust von Kunden (und in vielen Fällen Patienten) zustande kommt. Das sind enorme Summen – Geld, das eigentlich unter den Einnahmen verbucht würde. Um jedoch wirksame Gegenmaßnahmen entwickeln zu können, muss unbedingt klar sein, dass der Datendiebstahl in 8 von 10 Fällen auf ausgespähte Zugangsdaten zurückzuführen ist. Die Gefahr von Dritten unrechtmäßig in Erfahrung gebrachter Zugangsdaten darf deshalb nicht außer Acht gelassen werden, wenn in einem Unternehmen Maßnahmen zur Verstärkung der Zugriffskontrollen erwogen werden, um auch in Zukunft Telearbeit per Fernzugriff oder von unterwegs zu ermöglichen.

Und allen Inhabern mittelständischer Unternehmen, die sich gegen diese Art von Risiko gefeit fühlen, sei gesagt, dass sich im vergangenen Jahr jeder dritte Datendiebstahl in kleinen bis mittleren Unternehmen (KMUs) ereignete. Zwar fällt die Datenausbeute in KMUs für Kriminelle deutlich geringer aus als bei großen Konzernen, jedoch müssen in der Regel auch wesentlich weniger Hürden überwunden werden, um unbefugt Zugang zu wertvollen digitalen Daten zu erhalten, was häufig mittels Social Engineering geschieht. Und wie sich immer wieder zeigt, sind selbst kleine Unternehmen für Kriminelle absolut lukrativ.

Die mit Telearbeit erzielten Vorteile

Sollten Verantwortliche in den IT- und Sicherheitsabteilungen nun zu dem Schluss kommen, den Fernzugriff am besten zu verbieten, dürfen sie keinesfalls das übergeordnete Ziel des Unternehmens aus dem Blick verlieren: Teams in

7 von **10** sicherheitsrelevanten Angriffen betreffen mittelständische Unternehmen

Quelle: Global Security Report von Trustwave

3 von **4** Angriffe sind auf ausgespähte Zugangsdaten zurückzuführen

Quelle: DBIR-Studie von Verizon

1. The Global State of Information Security® Survey 2015, PwC, CIO und CSO: www.pwc.com/gsiss2015
2. US cybercrime: Rising risks, reduced readiness, PwC http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Gründe für den Ausbau der Telearbeit in Unternehmen:

- Geringere Kosten für Immobilien und Büroflächen
- Arbeitsplatzteilung – mehrere Mitarbeiter teilen sich einen Arbeitsplatz/-bereich
- Flexible, bedarfsgesteuerte Arbeitszeiten statt des traditionellen reglementierten Modells

Quelle: Forschung und Arbeit von Sandy Burud, PhD bei flexpaths.com

1 von 4 *Unternehmen in Nordamerika ermöglichen zumindest einigen Mitarbeitern Telearbeit*

die Lage versetzen, so produktiv wie möglich zu arbeiten. Sicherheit und Unternehmensstrategie müssen also Hand in Hand gehen, denn nur durch Produktivität und Flexibilität können Unternehmen und andere Organisationen weiter wachsen. Dabei muss unbedingt sichergestellt werden, dass Mitarbeiter jederzeit auf die von ihnen benötigten Daten und Services zugreifen können, unabhängig von dem verwendeten Gerät oder dem Ort, an dem sie sich gerade aufhalten. Wenn die Sicherheit allerdings erst im Nachhinein bedacht wird, werden Unternehmen früher oder später die Konsequenzen tragen müssen. Doch die Produktivität im Unternehmen zu hemmen, ist ebenfalls keine Lösung.

Obwohl virtuelle private Netzwerke (VPNs) weiterhin die beliebteste Lösung für einen sicheren Zugriff durch Telearbeiter sind, haben sich andere Technologien für den Fernzugriff in der Zwischenzeit als deutlich effektiver erwiesen. Dazu gehören Virtualisierungstechnologien, mit denen Anwendungen, spezielle Services oder komplette Desktop-Ansichten bereitgestellt werden können und die lediglich eine moderate Netzwerkbandbreite und Prozessorleistung beim Client-Gerät voraussetzen. Darüber hinaus halten sie private Daten zwar von den Remote-Geräten fern, ermöglichen aber dennoch den schnellen und einfachen Zugriff auf die benötigten Informationen. Je mehr diese Remote-Technologien in Unternehmen zum Einsatz kommen und von Mitarbeitern genutzt werden, desto höher steigen auch die Erwartungen. Die richtige Reaktion auf die Herausforderungen im Zusammenhang mit der Telearbeit kann also keine Ablehnung sein. Sie muss vielmehr darin bestehen, sich eingehend mit dem „Wie“ zu befassen.

Mitarbeiter ziehen Telearbeit dem Büroalltag vor

Ob Sie nun ein traditionelles VPN für Ihren Fernzugriff verwenden oder eine bestimmte Virtualisierungstechnologie – die Sicherheit hat oberste Priorität. Und da Datendiebstahl in 8 von 10 Fällen auf ausgespähte Zugangsdaten zurückzuführen ist, ist die sorgfältige Überprüfung der Identität des Benutzers die Grundlage für einen sicheren Fernzugriff.

Eine der wohl effektivsten Möglichkeiten zur Überprüfung der Identität ist die Zwei-Faktor-Authentifizierung. Oder anders ausgedrückt: eine Authentifizierungsmethode, bei der neben Zugangsdaten, die von unbefugten Dritten in

NetIQ verschafft Ihnen die Flexibilität, genau die Authentifizierungsmethode zu nutzen, die den Anforderungen Ihres Unternehmens am besten gerecht wird.

www.netiq.com

Erfahrung gebracht werden könnten, eines weiteres Merkmal abgefragt wird. Der Benutzer muss dann zur Authentifizierung beispielsweise einen Gerätecode angeben und seine Identität anschließend mit seinem Fingerabdruck, seinem Gesicht, seiner Stimme oder einem anderen Merkmal bestätigen. Bei ordnungsgemäßer Umsetzung hat sich ein mehrstufiger Authentifizierungsprozess als die wirksamste Methode erwiesen, um den Zugriff durch unbefugte Dritte zu verhindern.

Wenn Ihr Unternehmen für die Zwei-Faktor-Authentifizierung noch auf Hardtokens setzt, fallen wahrscheinlich zu hohe Lizenzgebühren und administrative Gemeinkosten an. Und wenn Sie nach und nach den Benutzerkreis der Telearbeiter in Ihrem Unternehmen erweitern, werden Sie früher oder später feststellen, dass Ihre bisherige Authentifizierungsmethode für VPN-Benutzer nicht skaliert – weder finanziell noch in Bezug auf den Administrationsaufwand. NetIQ kann Sie in beiden Bereichen unterstützen.

Wenn Sie den Fernzugriff auf sensible Daten per VPN oder mittels anderer Technologien nur mit Benutzeranmeldedaten schützen, spielen Sie mit dem Feuer. Und wenn Sie die jüngsten Schlagzeilen verfolgt haben, werden Sie zu dem Schluss kommen, dass Sie die Vernachlässigung Ihrer Sicherheit früher oder später teuer zu stehen kommen kann. Doch NetIQ kann Ihnen helfen. Dank der offenen Architektur und der unkomplizierten Benutzerlizenzierung ist das NetIQ Advanced Authentication Framework genau der Weg, den Sie einschlagen sollten.

Weitere Informationen zum Advanced Authentication Framework finden Sie unter www.netiq.com/2FA.

NetIQ
Deutschland
Fraunhoferstr. 7
85737 Ismaning
Tel: +49 (0)89 420940
Email: infoDE@netiq.com

Schweiz
Flughafenstrasse 90
P.O. Box 253 8058 Zürich
Tel: +41 (0)43 456 2400
Email: infoCH@netiq.com

info@netiq.com
www.netiq.com/communities
www.netiq.com

Die vollständige Liste unserer Niederlassungen in Nordamerika, Europa, Nahost, Afrika, Lateinamerika sowie im asiatisch-pazifischen Raum finden Sie unter: www.netiq.com/contacts

www.netiq.com

584-DE0020-001 | 11/16 | © 2016 NetIQ. Alle Rechte vorbehalten. NetIQ und das NetIQ Logo sind eingetragene Marken der NetIQ Corporation in den USA. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.