Rescue

IHR GUIDE FÜR EINEN SICHEREN FERNSUPPORT

Keine Chance für Cyberbedrohungen
beim Anwendersupport an jedem Ort

Überall sicheren Support geben

Die zunehmende Digitalisierung der Welt schürt Sorgen bei Unternehmen und Verbrauchern. Cyberkriminalität ist inzwischen ein hochprofessionelles Geschäft, Hackerangriffe nehmen zu. Daher fragen sich jetzt viele Unternehmen, wie sicher ihre Tools für die Remote-Arbeit sind.

Zusätzlich zu den bereits bekannten Sicherheitsanforderungen sind neue Bedrohungen aufgetaucht. In einer 2022 von GoTo beauftragten Umfrage hält knapp die Hälfte der Supportleiter (49 %) das Risiko von Cyberangriffen heute für höher als vor zwei Jahren. Die wichtigsten Zielanforderungen im Support sind ihrer Meinung nach ein abgesicherter Verbindungsaufbau und zuverlässige, sichere Supporttools für Techniker – beides jedoch nicht auf Kosten einer angenehmen Supporterfahrung für die Anwender.

Kommen Ihre aktuellen Fernsupporttools mit diesen Anforderungen zurecht?

Vergleichen Sie Ihre Lösung mit Rescue – unser Guide hilft Ihnen dabei.

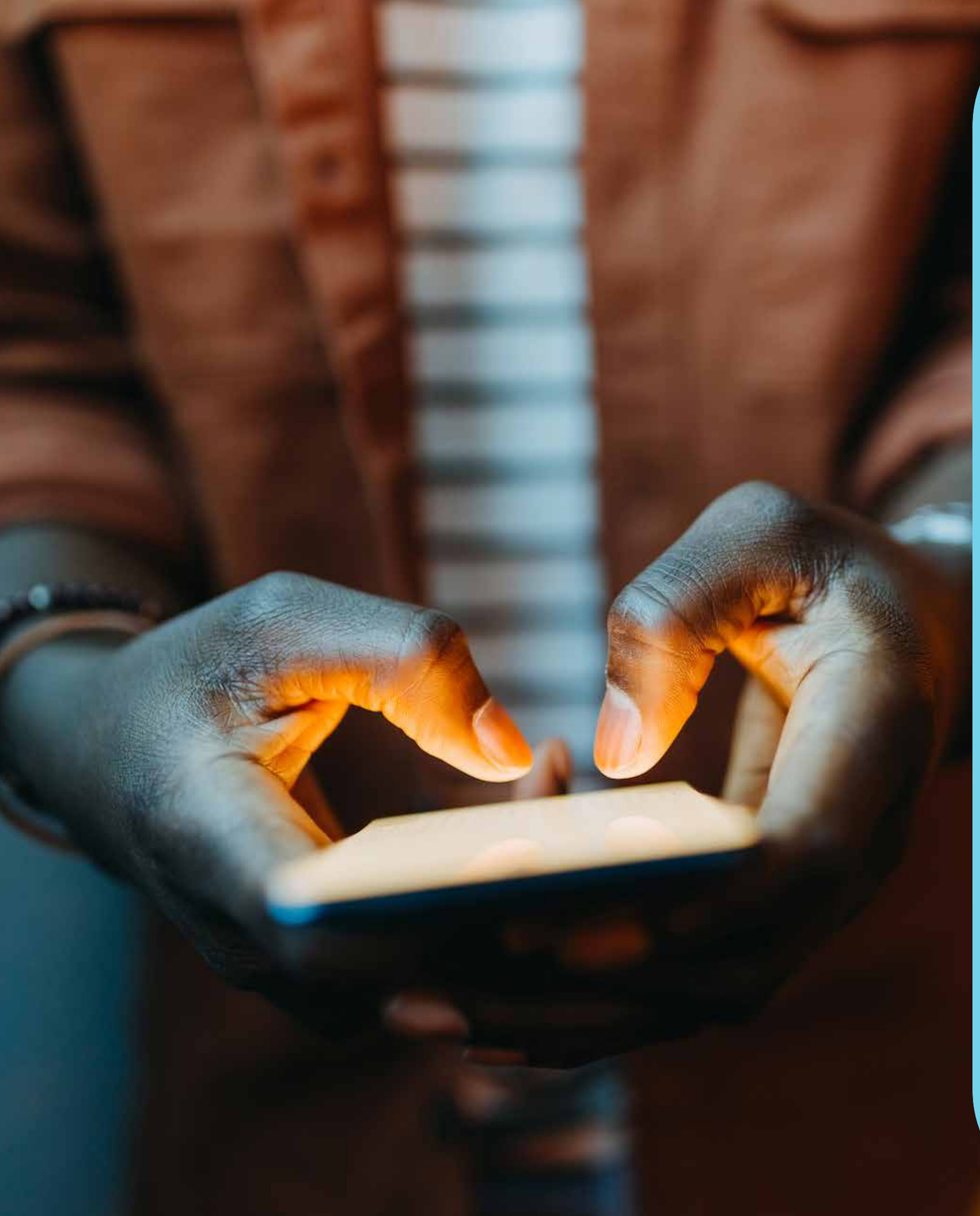
Quelle: IDG, Remote Customer Support Marketpulse Research für GoTo, Januar 2022.

Die wichtigsten Zielanforderungen im Support:

87 % Abgesicherte Remote-Verbindung

84 % Zuverlässige und sichere Supporttools

82 % Unkomplizierter Support



Vier wichtige Sicherheitsanforderungen bei der Remote-Verbindung zwischen Anwendern und Technikern:

1 Datenschutz

Audit Readiness: stets auf Prüfungen vorbereitet
Viele Unternehmen sind von externen Sicherheitsreports und Zertifizierungen abhängig, darunter SOC-2-Berichte (Service Organization Control 2) und die Einhaltung von Normen der ISO/IEC-27000-Reihe. Gehen Sie sicher, dass Ihr Lösungspartner SOC-2-Audits nach Typ II durchführen und Ihnen einen SOC-3-Bericht zukommen lässt und/oder ISO-27000-konform agiert.

Datenübermittlung nach strengsten Sicherheitsprotokollen
Ihre Fernsupportlösung sollte sich an den extrem hohen Sicherheitsstandards in der Finanzbranche ein Beispiel nehmen und Daten sowohl bei der Übermittlung als auch im ruhenden Zustand mittels TLS 1.2 (Transport Layer Security) und AES-256-Bit-Verschlüsselung schützen.

Multifaktor-Authentifizierung
Wenn Sie die zweistufige Verifizierung verwenden, können Unbefugte nicht auf Ihr Fernsupporttool zugreifen. Active Directory, das Single Sign-On und die Benutzersynchronisierung unterstützt, hilft Ihnen, jede einzelne Anmeldung zu schützen. Außerdem sollten sich Technikerkonten nach Bedarf aktivieren bzw. deaktivieren lassen.

2 Sichere Verbindungsmethoden

Selbst gehostete PIN-Seite
Ihre Fernsupportlösung sollte Ihnen die Möglichkeit geben, Ihre PIN-Eingabeseite selbst zu hosten. Dann müssen Sie Anwender nicht auf die öffentliche PIN-Seite weiterleiten, und Sie können die Seite an Ihre Marke anpassen und optional weitere Sicherheitsebenen hinzufügen.

Validierung des Unternehmens-PIN-Codes
Bei dieser Art von Validierung akzeptiert die Supportlösung nur von Ihrem Konto generierte PINs; Codes aus anderen Quellen funktionieren nicht. Dadurch können nur Ihre eigenen Techniker auf die Computer der Anwender zugreifen. Für zusätzlichen Schutz lassen sich die PIN-Codes sperren, sodass sie nur auf Ihrer Website oder über eine Verknüpfung auf dem Anwender-Desktop funktionieren.

Domain-Validierung
Es kann vorkommen, dass Kriminelle mit dem HTML-Code Ihrer PIN-Seite eine eigene „Dummy“-Seite erstellen. Bei der Domain-Validierung wird überprüft, ob der HTML-Code des PIN-Eingabe- oder Kanalformulars mit den in der Supportlösung vorab genehmigten Domains übereinstimmt. So können Unbefugte keine Benutzerdaten in Erfahrung bringen.

IP-Adressen-Beschränkungen
Gehen Sie sicher, dass Ihre Techniker auch im Homeoffice die Unternehmensrichtlinien einhalten. Wenn Sie IP-Adressen-Beschränkungen einrichten, können sich die Techniker nur innerhalb Ihres VPNs/Netzwerks oder einer Liste zulässiger IP-Bereiche bei der Fernsupportlösung anmelden.

Paket mit Zugriffsbeschränkungen
Diese Option geht über die IP-Adressen-Beschränkungen hinaus. Sie stellt sicher, dass Anwender innerhalb Ihres VPNs/Netzwerks nur mit von Ihrem Konto generierten PIN-Codes Support erhalten können. Alternativ können Sie Einschränkungen für Techniker festlegen, damit diese nur für Anwender in einem bestimmten IP-Bereich Support leisten können.

Zugriff nur von bestimmten Domains
Ihre Fernsupportlösung sollte sich so konfigurieren lassen, dass Ihre Anwender nur von in der Firewall zugelassenen Domains aus Support erhalten können. Zugriffe von anderen Domains aus auf ihren Computer werden unterbunden.

Geben Sie Anwendern ein sicheres Gefühl

Das Vertrauen der Endanwender ist genauso wichtig wie die Features und Funktionen Ihres Remote-Supporttools. Die Möglichkeit, Ihr Logo zum Supporterlebnis hinzuzufügen, lässt sie wissen, dass sie an der richtigen Stelle sind, um Hilfe zu erhalten.

Passen Sie Folgendes an:

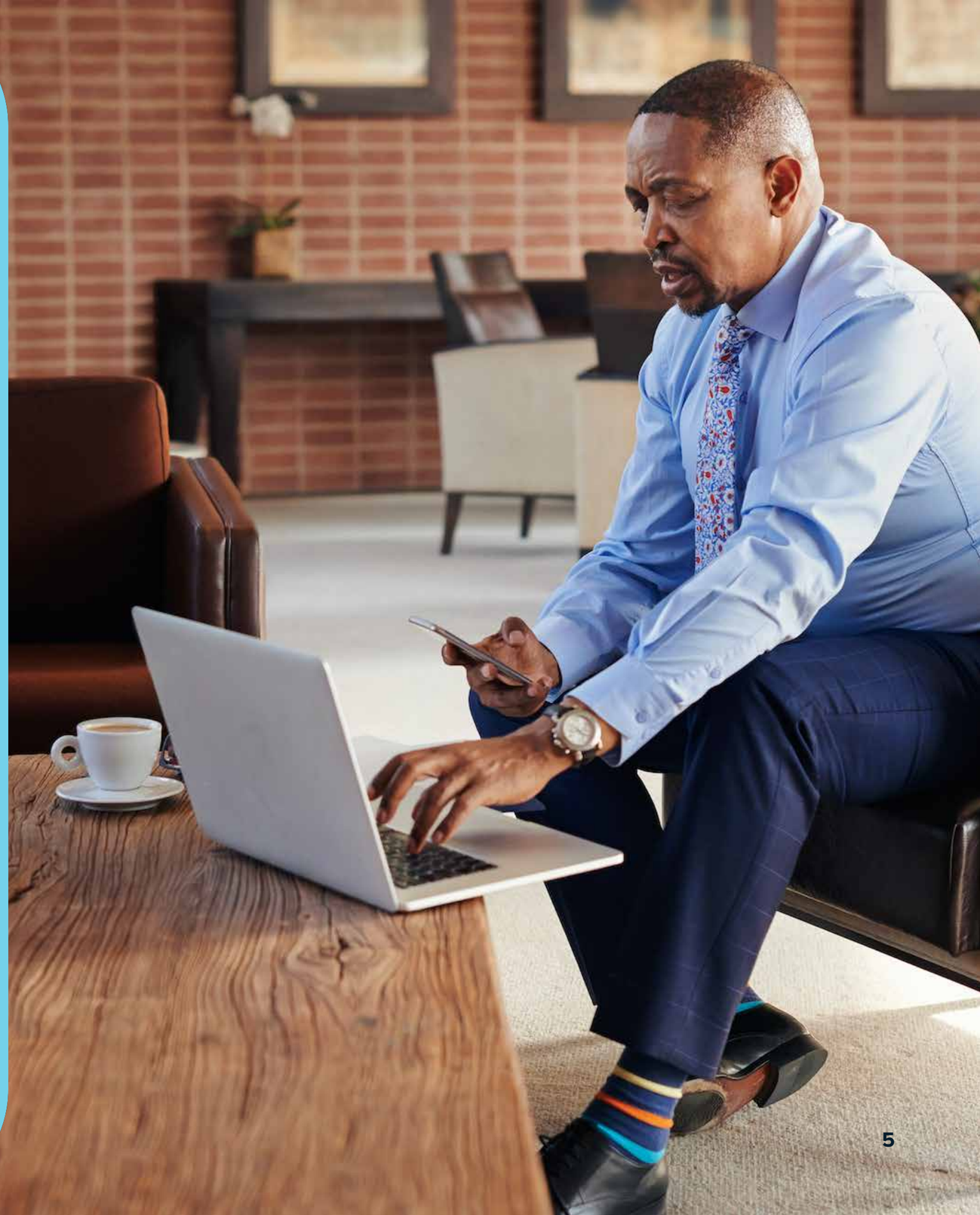
- PIN-Eingabeseite
- herunterladbares Applet
- Desktopsymbol

3 Zuverlässige Verwaltung

Technikerverwaltung, Rollen und Berechtigungen
Bei der Verwaltung des Technikerzugriffs werden die Rollen und Berechtigungen festgelegt, die jeder Techniker für seine Arbeit braucht. Ihre Administratoren müssen den einzelnen Technikergruppen Berechtigungen zuweisen können, damit diese Geräte remote steuern, Dateien übertragen oder Echtzeit-Nutzungsberichte abrufen können.

Tiefgehende Einblicke
Wenn Sie Einblick in die Leistung Ihrer Fernsupportlösung und Ihrer Techniker haben, wissen Sie, wie Sie Ihren Service weiter verbessern können – und dass Ihre Daten geschützt sind. Halten Sie nach einer Fernsupportlösung mit umfassenden Audit-, Protokollierungs- und Berichtsfunktionen Ausschau.

Berechtigungsbasierter Zugriff
Wenn der Anwender dem Supporttechniker explizit eine Genehmigung erteilen muss, gibt ihm das nicht nur ein sicheres Gefühl, sondern es schützt auch Ihr Unternehmen. Techniker sollten nur mit der Zustimmung der Anwender auf deren Geräte zugreifen können.



4 Keine Kompromisse bei der Compliance

DSGVO (je nach Standort)
Ihre Fernsupportlösung muss Ihnen die Kontrolle über die gespeicherten Daten geben, damit Sie die Vorgaben der Datenschutz-Grundverordnung (DSGVO) einhalten können.

HIPAA (je nach Branche)
Ihre Supportlösung hat zwar keine Kontrolle über die während einer Supportsitzung von den Anwendern ausgetauschten Inhalte, sollte aber so konzipiert sein, dass sie strengste Sicherheitsrichtlinien erfüllt und Einrichtungen, die den Datenschutzauflagen des US-amerikanischen Health Insurance Portability and Accountability Acts (HIPAA) unterliegen, bei der Einhaltung der entsprechenden regulatorischen Vorgaben hilft.

Sicheres Arbeiten und sicherer Support – an jedem Ort.

Vom abgesicherten Verbindungsaufbau bis zur nahtlosen Fehlerbehebung – mit einem sicheren Fernsupporttool, auf das Sie sich verlassen können, sparen Sie Nerven. Mit Rescue halten Sie auch strengste Sicherheitsvorgaben ein und schützen Ihre Anwender und Ihr Unternehmen.

Rescue, von GoTo.
Remote-Support leicht gemacht

12.27.2022/GoTo0550/PDF