

Stellen Sie sicher, dass nur als vertrauenswürdig eingestufte Endgeräte auf Ihr Unternehmensnetz zugreifen können

- **Bestimmen Sie über einen einzigartigen Identifikationsprozess, ob Endgeräte vertrauenswürdig sind**
- **Stellen Sie sicher, dass nur vom Unternehmen angegebene oder autorisierte Endgeräte auf das Netz zugreifen**
- **Überprüfen Sie bei der VPN-Authentifizierung zusätzlich die Identität des Endgeräts**
- **Überprüfen Sie Endgerät- und Nutzerverhalten anhand ausführlicher Berichte und Prüfprotokolle**

Ihr IT-Personal hat – zu Recht – große Bedenken bezüglich der Sicherheit. Betrügerische Praktiken, wie z. B. Diebstahl von Passwörtern, Manipulation der Identität und Replay-Angriffe, lassen IT-Experten darüber im Unklaren, wer zu einer bestimmten Zeit auf das Netz zugreift. Selbst die zuversichtlichsten IT-Manager bezweifeln, dass nicht autorisierte Endgeräte daran gehindert werden können, die Kommunikation abzufangen oder in das Unternehmen einzudringen.

Die beste Methode zum Aufbau vertrauenswürdiger Verbindungen besteht in einer leistungsstarken Authentifizierung basierend auf mehreren Faktoren. Allerdings war es bisher so, dass jede neue Sicherheitsebene ein Mehr an Kosten, Verwaltungsaufwand und Schwächen zur Folge hatte, über die Sicherheitsrichtlinien wiederum problemlos umgangen werden konnten.

Zum Glück gibt es eine neuartige Methode, um eine Mehrfaktor-Authentifizierung zu erreichen und sich dieser Herausforderung zu stellen. Diese Methode heißt DeviceID. Sie ist innovativ und preisgünstig und wird von iPass, einem Marktführer für „kompromisslos sichere Verbindungen“ bereitgestellt.

Erhöhen Sie die Netzsicherheit durch Mehrfaktor-Authentifizierung

DeviceID unterstützt IT-Manager beim Erstellen und Durchsetzen von Zugriffsregeln, mit denen sichergestellt wird, dass nur die Endgeräte über ein VPN auf das Netz zugreifen können, die vom Unternehmen autorisiert wurden. Durch die patentierte, softwarebasierte Authentifizierungstechnologie wissen Sie genau, welche Endgeräte auf Ihr Unternehmensnetz zugreifen wollen. Auf Grund seiner besonderen Fähigkeit, die firmeneigenen Bestände von persönlichen Endgeräten oder völlig unbekanntem Computern zu unterscheiden, kann DeviceID eine wertvolle Rolle bei der Identitäts-, Zugriffs- und Regelverwaltung spielen.

DeviceID ist eine zusätzliche Methode, mit der iPass es Ihnen ermöglicht, Regeln in Kraft zu setzen, die die Sicherheit von Endgeräten erhöhen, ohne die Produktivität der Nutzer zu behindern oder die Verwaltung für das IT-Personal zu erschweren.

- **Dynamische Endgeräteabfrage:** Identifiziert Endgeräte durch eine Überprüfung verschiedener Hardware-Attribute bei allen Authentifizierungsanforderungen, schützt vor Replay-Angriffen, Reverse Engineering und Manipulation.
- **Datenverschlüsselung auf Endgeräten:** Codiert alle Hardwaredaten, bevor diese über einen sicheren Kanal übertragen und zu Vergleichs- und Überprüfungszwecken auf geschützten Authentifizierungsservern gespeichert werden.
- **Leistungsstarke Zweifaktor-Authentifizierung:** Kombiniert die Endgeräteidentifikation mit einem Usernamen und einem Passwort, um den Netzzugriff auf autorisierte Endgeräte und authentifizierte Nutzer zu beschränken. Es ist keine teure Zusatzhardware oder komplexe software-basierte Lösung erforderlich.

Setzen Sie Sicherheitsregeln für Endgeräte in Kraft

DeviceID ermöglicht es Ihnen, die Vertrauenswürdigkeit von Endgeräten herzustellen. Durch die Integration einer gerätebasierten Authentifizierung können Sie eine strengere Zugriffskontrolle anwenden und die Einhaltung von Sicherheitsregeln für Endgeräte im gesamten Netz durchsetzen. Mit einer Regelverwaltung auf Gerätebasis können Sie den Netzzugriff mobiler Nutzer auf der Grundlage einer Kombination zweier Kriterien steuern, nämlich auf der Identität des Nutzers und auf dem von ihm verwendeten Endgerät. So kann die IT-Abteilung z. B. den privaten PC eines Angestellten als „weniger vertrauenswürdig“ einstufen als ein Firmen-Notebook.

DeviceID kann nicht nur zur Definition von Vertrauensebenen für verschiedene Endgeräte verwendet werden, sondern auch zur Stärkung des VPN-Authentifizierungsprozesses beitragen. Eine „One-Click-Integration“ in führende VPN-Produkte ermöglicht einen sicheren und lückenlosen Zugriff, bei dem nicht nur die Identität des Endgeräts überprüft, sondern auch der Nutzer authentifiziert wird. Somit unterstützt DeviceID das Unternehmensziel – den Schutz des Unternehmensnetzes –, indem die Integrität der daran angeschlossenen Endgeräte gewährleistet wird.

Endgeräte-Identität und transparente Durchsetzung senken die Gesamtbetriebskosten

Früher gingen mit dem Hinzufügen weiterer Sicherheitsebenen höhere Verwaltungskosten und eine geringere Produktivität der Nutzer einher, weil sie sich oftmals erst in den Gebrauch dieser Technologien einarbeiten mussten. Mit DeviceID können Sie eine leistungsstarke Zweifaktor-Authentifizierung einführen, die eine Durchsetzung im Hintergrund ermöglicht, ohne dass die Produktivität der Nutzer darunter leidet. Anders als bei digitalen Zertifikaten gibt es bei DeviceID-Nutzern keine Hardwarekomponenten oder Token, die geknackt werden, verloren gehen oder Ärger bereiten können, denn auf dem PC gibt es für Hacker nichts, was kopiert oder exportiert werden könnte.

Für die IT-Abteilung wird die Verwaltung von DeviceID durch ein robustes Webportal erleichtert, mit welchem sich Reports in Echtzeit erstellen lassen. Verfassen Sie detaillierte Berichte, um zu erfahren, welche authentifizierten Endgeräte zurzeit auf das Netz zugreifen. Verfolgen Sie die Netzwerkaktivität nach Nutzer und Endgerät, um über Prüfberichte Einsicht in Verwendung und Missbrauch zu erhalten, was bei der Einhaltung rechtlicher Auflagen hilfreich sein kann.

- **Einfache Implementierung und Verwendung:** Machen Sie die Implementierung für IT-Personal wie Endnutzer durch eine transparente Registrierung und Aktivierung so einfach wie möglich. Laden Sie Nutzer aus bestehenden Datenbanken hoch; verteilen, installieren und aktivieren Sie die DeviceID-Software im Hintergrund.
- **Einfache Verwaltung:** Verwenden Sie ein intuitives Webportal, um eindeutige Merkmale von Endgeräten einzurichten, Zugriffsregeln zu definieren, Nutzerprofile zu verwalten und die Verwendung des Netzes zu überwachen.
- **Berichterstellung in Echtzeit:** Generieren und filtern Sie Berichte nach Nutzer, Endgerät, Transaktionstyp und Status, um differenziert steuern zu können, wer über welches Endgerät auf das Netz zugreifen kann. Berichte werden direkt aus der DeviceID-Datenbank extrahiert, sodass ein vollständiges Prüfprotokoll aller Netzwerkaktivitäten gewährleistet ist.
- **Transparente Authentifizierung:** Ermöglichen Sie eine Authentifizierung auf Geräteebene durch den Autorisierungsprozess, mit dem die Nutzer bereits vertraut sind. Da sich durch DeviceID für die Endnutzer nichts ändert, entfallen Nutzerinteraktionen, Lernprozesse und Schulungen.
- **Software-basierte Lösung:** Kontrollieren Sie die Kosten für Hardware und Support durch eine software-basierte Lösung, die eine leistungsstarke Authentifizierung ohne zusätzliche Hardware, wie Token, Kartenlesegeräte oder Biometriegeräte, ermöglicht.

Vertrauen leicht gemacht

Die iPass-Plattform bietet bereits Passwortverschlüsselung, SSL-Tunneling, Integration mit bestehenden VPNs, digitale Zertifikate und Funktionen zur Durchsetzung von Regeln, um Ihre Nutzer und die Daten Ihres Unternehmens zu schützen. DeviceID erweitert dies alles um eine weitere wertvolle Sicherheitsebene. Diese Erweiterung der iPass-Services erhöht die Sicherheit sowohl auf Remote- als auch auf Unternehmensebene, während die Produktivität der mobilen Nutzer erhalten bleibt. Weitere Informationen darüber, wie DeviceID von iPass „kompromisslos sichere Verbindungen“ bereitstellt, finden Sie unter www.ipass.de – oder sprechen Sie noch heute mit Ihrem iPass-Betreuer!

Systemanforderungen

Unterstützte Plattformen:

Microsoft Windows 2000
Microsoft Windows XP

Unterstützte VPNs:

Nortel Contivity
Cisco Concentrator

Serversoftware:

Microsoft Windows 2000 mit Service Pack 4 oder Microsoft Windows 2000 Advanced Server mit Service Pack 3
Oracle 9i
Microsoft IIS für Adminportal erforderlich
Internet Explorer ab Version 6.0 für Adminportal erforderlich

iPass EMEA
Region D/A/CH
Wiener Platz 7
D-81667 München
www.ipass.de

© Copyright 2004 iPass Inc. Alle Rechte vorbehalten. iPass und das iPass-Logo sind eingetragene Marken der iPass Inc.; DeviceID ist eine Marke der iPass Inc. Alle anderen Namen von Unternehmen oder Produkten können Marken der entsprechenden Firmen sein. Es wurde jede nur mögliche Anstrengung unternommen, um die Richtigkeit der bereitgestellten Informationen zu gewährleisten; iPass übernimmt jedoch keine Haftung für eventuelle Fehler. Die Spezifikationen und sonstigen Informationen dieses Dokuments können ohne Vorankündigung geändert werden.

PRDBF-DID
113004