ข้อมูลด้านความปลอดภัยของ TeamViewer

กลุ่มเป้าหมาย

เอกสารฉบับนี้มีจุดมุ่งหมายเพื่อผู้ดูแลระบบเครือข่ายมืออาชีพ
ข้อมูลในเอกสารฉบับนี้ค่อนข้างเป็นข้อมูลทางเทคนิคและมีรายละเอียดจำนวนมาก จากข้อมูลนี้ มืออาชีพด้าน IT จะได้รับภาพรายละเอียดของมาตรฐานด้านความปลอดภัยของ TeamViewer และกำจัดข้อวิตกกังวลใดๆ ก่อนเริ่มใช้งานซอฟต์แวร์ของเรา
โปรดแจกจ่ายเอกสารฉบับนี้ให้กับลูกค้าของคุณเพื่อลดข้อวิตกกังวลด้านความปลอดภัยใดๆ ที่อาจมี

หากคุณไม่ได้มองว่าตนเองเป็นส่วนหนึ่งของกลุ่มเป้าหมาย ข้อมูลทั่วไปในหัวข้อ บริษัท / ซอฟต์แวร์ จะช่วยให้คุณเห็นภาพได้ชัดเจนยิ่งขึ้นเช่นกันว่าเราให้ความสำคัญในเรื่องความปลอดภัย

บริษัท / ซอฟต์แวร์

เกี่ยวกับเรา

TeamViewer GmbH ก่อตั้งในปี 2005 โดยตั้งอยู่ทางตอนใต้ของประเทศเยอรมนี ในเมืองเกิพพิงเง่น (ใกล้ชตุทท์การ์ท) และมีบริษัทย่อยอยู่ในประเทศออสเตรเลียและสหรัฐอเมริกา เราพัฒนาและจำหน่ายระบบที่มีความปลอดภัยสำหรับความร่วมมือบนเว็บเท่านั้น ภายในช่วงเวลาสั้นๆ สิทธิ์ใช้งาน Freemium ของเราเติบโตขึ้นอย่างรวดเร็ว โดยมีผู้ใช้ซอฟต์แวร์ TeamViewer มากกว่า 200 ล้านคน บนอุปกรณ์มากกว่า 1.4 พันล้านเครื่อง ในมากกว่า 200 ประเทศทั่วโลก ซอฟต์แวร์พร้อมให้บริการมากกว่า 30 ภาษา

ความเข้าใจของเราในด้านความปลอดภัย

ในทุกช่วงเวลา TeamViewer มีผู้ใช้งานมากกว่า 30 ล้านคน ผู้ใช้เหล่านี้ได้รับการสนับสนุนบนอินเทอร์เน็ตทันที ซึ่งรวมถึงการเข้าถึงคอมพิวเตอร์ที่ไม่ต้องมีผู้เฝ้าดู (เช่น การสนับสนุนระยะไกลสำหรับเซิร์ฟเวอร์) และการจัดประชุมออนไลน์ สามารถใช้ TeamViewer ในการควบคุมคอมพิวเตอร์อื่นจากระยะไกลได้ราวกับว่าคุณนั่งอยู่หน้าคอมพิวเตอร์เครื่องนั้นเอง ทั้งนี้ขึ้นอยู่กับการกำหนดค่า หากผู้ใช้ที่เข้าระบบในคอมพิวเตอร์ระยะไกลเป็นผู้ดูแลระบบ Windows, Mac หรือ Linux ผู้ใช้คนดังกล่าวจะได้รับสิทธิ์ผู้ดูแลระบบบนคอมพิวเตอร์เครื่องดังกล่าวด้วยเช่นกัน

แน่นอนว่าฟังก์ชันการทำงานอันทรงพลังบนอินเทอร์เน็ตที่อาจมีความเสี่ยงในเรื่องความปลอดภัยจะต้องได้รับการปกป้องจากภัยคุกคามต่างๆ อย่างมาก ที่จริงแล้ว ปัจจัยเรื่องความปลอดภัยมีความสำคัญเหนือเป้าหมายการพัฒนาผลิตภัณฑ์ทั้งหมดของเราและเป็นสิ่งที่เราอยู่ในสายเลือดของเรา เราต้องการทำให้มั่นใจได้ว่าการเข้าถึงคอมพิวเตอร์ของคุณมีความปลอดภัย รวมถึงปกป้องผลประโยชน์ของเราเองด้วย
เนื่องจากผู้ใช้นับล้านคนทั่วโลกจะเชื่อมั่นโซลูชันที่มีความปลอดภัยเท่านั้นและมีเพียงโซลูชันที่ปลอดภัยเท่านั้นที่จะสามารถสร้างความสำเร็จทางธุรกิจระยะยาวให้กับเราได้

การประเมินของผู้เชี่ยวชาญภายนอก

ซอฟต์ แวร์ TeamViewer ของเราได ้ รับตราสัญลักษณ์ คุณภาพห ้ าดาว (สูงสุด) จากสมาคมผู้เชี่ยวชาญและผู้ตรวจทานด ้ าน IT (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.) ผู้ตรวจทานอิสระของ BISG e.V. จะตรวจสอบผลิตภัณฑ์ ต่ างๆ ของผู้ผลิตเกี่ยวกับคุณลักษณะทางด ้ านคุณภาพ ความปลอดภัย และบริการ

ข ้ อมูลอ ้ างอิง

ปัจจุบัน TeamViewer มีผู้ใช้งานมากกว่า 200 ล้านคน องค์กรชั้นนำระดับโลกจากทุกอุตสาหกรรม (รวมถึงธุรกิจที่เกี่ยวข้องกับข้อมูลความลับ เช่น การธนาคาร การเงิน การดูแลสุขภาพ และรัฐบาล) ใช้งาน TeamViewer อย่างประสบความสำเร็จ

โปรดอ่านข้อมูลอ้างอิงของเราที่สามารถพบเห็นได้บนอินเทอร์เน็ต เพื่ออ่านความประทับใจเกี่ยวกับโซลูชันของเรา คุณจะพบว่าบริษัทอื่นๆ ส่วนใหญ่มีข้อกำหนดด้านการรักษาความปลอดภัยและความพร้อมใช้งานที่คล้ายคลึงกัน และหลังจากที่ได้ตรวจสอบอย่างละเอียดถี่ถ้วนแล้ว บริษัทเหล่านั้นได้หันมาใช้งาน TeamViewer โปรดอ่านรายละเอียดทางเทคนิคในเอกสารส่วนที่เหลือ เพื่อสร้างความประทับใจของคุณเอง

เซสชัน TeamViewer

การสร้างเซสชันและประเภทของการเชื่อมต่อ

ในการสร้างเซสชัน TeamViewer จะกำหนดประเภทการเชื่อมต่อที่เหมาะสมที่สุด หลังจากทำความรู้จักผ่านเซิร์ฟเวอร์หลักของเราแล้ว จะมีการสร้างการเชื่อมต่อโดยตรงผ่าน UDP หรือ TCP ใน 70% ของคำขอทั้งหมด (แม้จะอยู่เบื้องหลังเกตเวย์มาตรฐาน NAT และไฟร์วอลล์ก็ตาม) และการเชื่อมต่อที่เหลือจะถูกกำหนดเส้นทางผ่านเครือข่ายเราเตอร์ที่สำรองการทำงานได้ดีผ่าน TCP หรือการทันเนล https โดยที่คุณไม่ต้องเปิดพอร์ตใดๆ เพื่อทำงานกับ TeamViewer

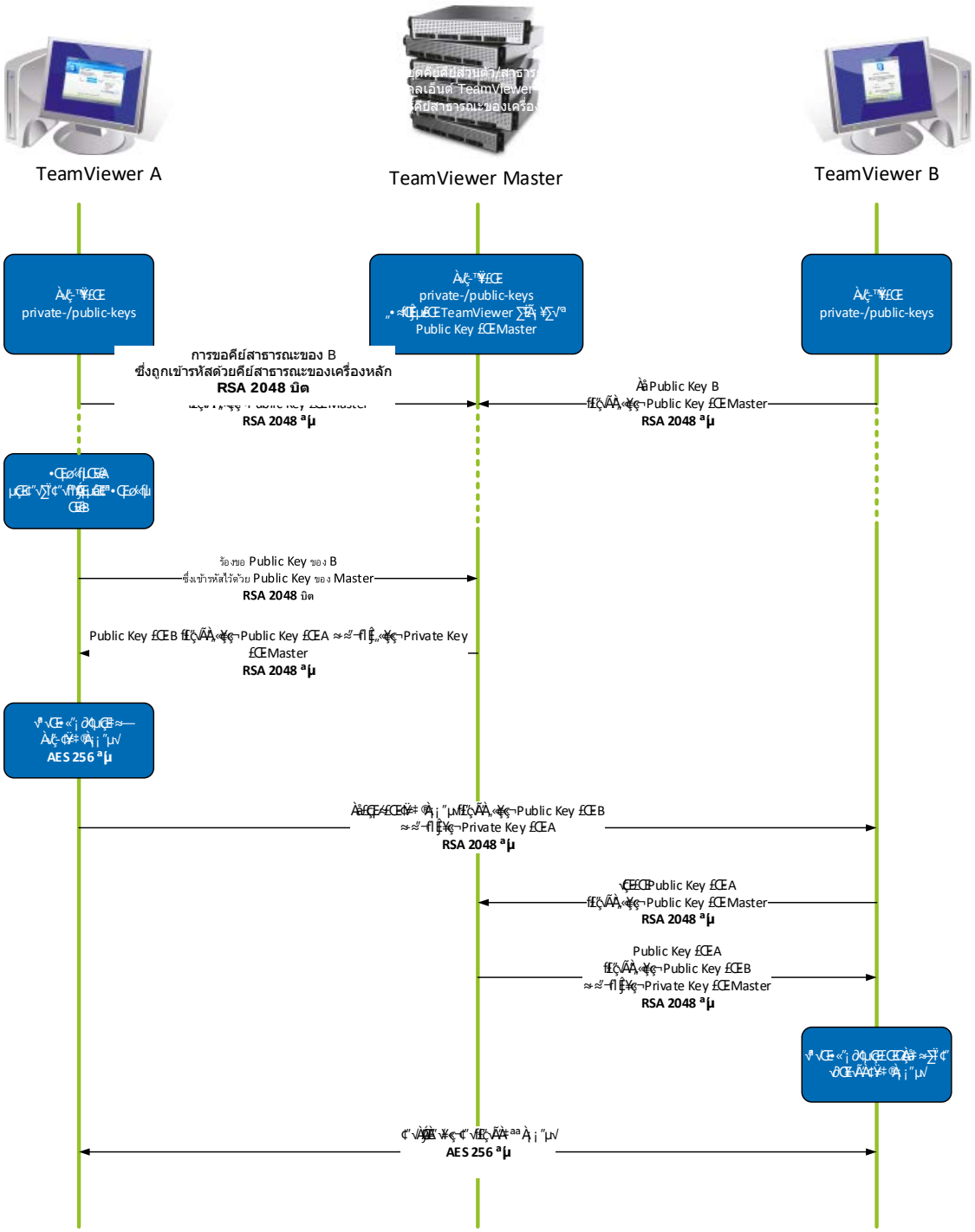
ซึ่งจะอธิบายต่อไปในย่อหน้าการเข้ารหัสและการรับรองความถูกต้อง
และแม้แต่เราเองซึ่งเป็นผู้ให้บริการเราดิ้งเซิร์ฟเวอร์ก็ไม่สามารถอ่านปริมาณการใช้งานข้อมูลที่เข้ารหัสได้

การเข้ารหัสและการรับรองความถูกต้อง

TeamViewer Traffic มีการรักษาความปลอดภัยด้วยการแลกเปลี่ยนคีย์สาธารณะ/ส่วนตัว RSA และการเข้ารหัสเซสชัน AES (256 บิต) มีการใช้เทคโนโลยีนี้ในรูปแบบที่คล้ายคลึงกันสำหรับ http/SSL ซึ่งนับว่ามีความปลอดภัยที่สุดในมาตรฐานปัจจุบัน เนื่องจากคีย์ส่วนตัวจะไม่ออกจากคอมพิวเตอร์ไคลเอ็นต์ กระบวนการนี้จะช่วยทำให้มั่นใจได้ว่าคอมพิวเตอร์ที่เชื่อมต่อระหว่างกันซึ่งรวมถึงเราดิ้งเซิร์ฟเวอร์ TeamViewer จะไม่สามารถถอดรหัสของกระแสข้อมูลได้

ไคลเอ็นต์ TeamViewer แต่ละหน่วยได้ดำเนินการคีย์สาธารณะของคลัสเตอร์หลักเรียบร้อยแล้ว จึงสามารถเข้ารหัสข้อความไปยังคลัสเตอร์หลักและตรวจสอบข้อความที่ผ่านการรับรองแล้วได้ PKI (Public Key Infrastructure - โครงสร้างพื้นฐานของคีย์สาธารณะ) ป้องกันการโจมตีผ่านคนกลางได้อย่างมีประสิทธิภาพ แม้ว่าจะมีการเข้ารหัส แต่จะไม่มีการส่งรหัสผ่านโดยตรง โดยจะส่งผ่านกระบวนการการตอบกลับของการตรวจสอบและบันทึกไว้บนคอมพิวเตอร์เฉพาะที่เท่านั้น

ในระหว่างการรับรองความถูกต้อง จะไม่มีการส่งรหัสผ่านโดยตรงเนื่องจากใช้โปรโตคอล Secure Remote Password (SRP) และมีเพียงตัวตรวจสอบรหัสผ่านเท่านั้นที่ถูกจัดเก็บไว้ในคอมพิวเตอร์เฉพาะที่



การเข้ารหัสและการรับรองความถูกต้องของ TeamViewer

การตรวจสอบความถูกต้องของ TeamViewer ID

TeamViewer ID ขึ้นอยู่กับคุณลักษณะของฮาร์ดแวร์และซอฟต์แวร์ต่างๆ และจะถูกสร้างขึ้นโดย TeamViewer โดยอัตโนมัติ เซิร์ฟเวอร์ TeamViewer จะตรวจสอบความถูกต้องของ ID เหล่านี้ก่อนการเชื่อมต่อทุกครั้ง

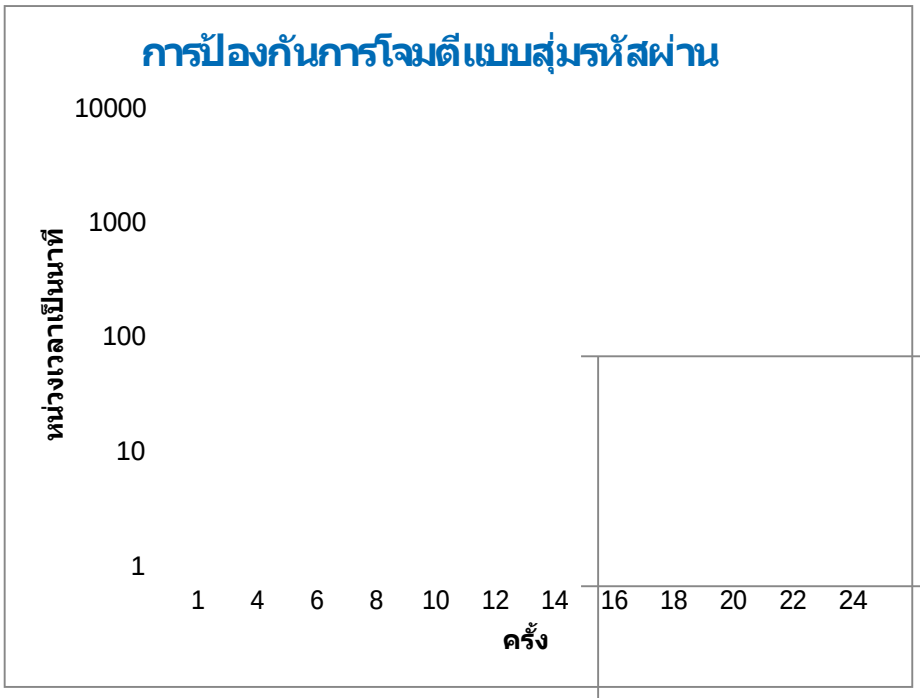
การปกป้องจากการโจมตีแบบสุ่มรหัสผ่าน

ลูกค้าที่ขอข้อมูลเกี่ยวกับความปลอดภัยของ TeamViewer มักจะสอบถามในเรื่องการเข้ารหัส ซึ่งเป็นเรื่องปกติที่ความเสี่ยงในเรื่องบุคคลภายนอกจะสามารถตรวจสอบการเชื่อมต่อได้หรือการถูกเจาะข้อมูลการเข้าถึง TeamViewer จะเป็นสิ่งที่ผู้คนหวาดกลัวมากที่สุด แต่ความจริงแล้ว การโจมตีแบบดั้งเดิมมักมีความอันตรายมากที่สุด

ในบริบทด้านความปลอดภัยของคอมพิวเตอร์
การโจมตีแบบสุ่มรหัสผ่านเป็นการลองผิดลองถูกในการเดารหัสผ่านที่ปกป้องทรัพยากรหนึ่งๆ อยู่ด้วยพลังการประมวลผลที่เพิ่มมากขึ้นของคอมพิวเตอร์มาตรฐานทั่วไป จึงลดเวลาในการคาดเดารหัสผ่านยาวๆ ลงได้อย่างมาก

โดยในการป้องกันการโจมตีแบบสุ่มรหัสผ่าน TeamViewer ได้เพิ่มการหน่วงเวลาในระหว่างที่มีการพยายามเชื่อมต่อ จึงต้องใช้เวลานานถึง 17 ชั่วโมงสำหรับการพยายาม 24 ครั้ง เวลาแฝงจะถูกรีเซ็ตหลังจากที่มีการป้อนรหัสผ่านที่ถูกต้องเท่านั้น

TeamViewer ไม่เพียงแค่มีกลไกในการปกป้องลูกค้าจากการถูกโจมตีจากคอมพิวเตอร์เครื่องใดเครื่องหนึ่งเท่านั้น แต่ครอบคลุมคอมพิวเตอร์หลายเครื่องซึ่งเรียกว่าการโจมตีของบอตเน็ต ที่พยายามจะเข้าถึง TeamViewer ID ใดๆ โดยเฉพาะ



ตาราง: เวลาที่ใช้หลังจากการพยายามเชื่อมต่อ n ครั้งระหว่างการโจมตีแบบสุ่มรหัสผ่าน

การรับรองรหัส

สำหรับคุณลักษณะเพิ่มเติมในด้านความปลอดภัย
ซอฟต์แวร์ทั้งหมดของเราผ่านการรับรองรหัส VeriSign
ซึ่งหมายความว่าสามารถระบุผู้พิมพ์ซอฟต์แวร์ได้เสมอ
หากมีการเปลี่ยนแปลงซอฟต์แวร์ในภายหลัง ลายเซ็นดิจิตอลจะใช้ไม่ได้โดยอัตโนมัติ

ศูนย์ข้อมูลและแกนหลัก

เพื่อมอบความปลอดภัยและความพร้อมในการให้บริการ TeamViewer ที่ดีที่สุด เซิร์ฟเวอร์ TeamViewer ทั้งหมดตั้งอยู่ในศูนย์ข้อมูลซึ่งเป็นไปตามมาตรฐาน ISO 27001 และยกระดับการเชื่อมต่อของผู้ให้บริการซึ่งมีการสำรองการทำงานหลายชั้นและมีอุปกรณ์จ่ายไฟสำรอง รวมทั้งมีการใช้งานฮาร์ดแวร์ที่มีชื่อเสียงและล้ำสมัยเท่านั้น
และเซิร์ฟเวอร์ทั้งหมดที่จัดเก็บข้อมูลสำคัญตั้งอยู่ภายในประเทศเยอรมนีหรือออสเตรีย

การได้รับการรับรอง ISO 27001 หมายถึงมีการควบคุมการเข้าถึงส่วนบุคคล การติดตั้งกล้องวงจรปิด การตรวจจับการเคลื่อนไหว
การจัดให้มีพนักงานรักษาความปลอดภัยประจำสถานที่คอยติดตามดูแลตลอดเวลาจะช่วยให้มั่นใจได้ว่าการเข้าถึงศูนย์ข้อมูลเป็นสิทธิ์ของผู้ที่ได้อนุญาตเท่านั้นและรับรองว่ามีการรักษาความปลอดภัยฮาร์ดแวร์และข้อมูลอย่างดีที่สุด และยังมีการตรวจสอบรหัสประจำตัวอย่างละเอียดถี่ถ้วนบริเวณทางเข้าออกศูนย์ข้อมูลซึ่งมีเพียงแห่งเดียว

บัญชี TeamViewer

บัญชี TeamViewer ถูกจัดเก็บไว้บนเซิร์ฟเวอร์ TeamViewer โดยเฉพาะ สำหรับข้อมูลเกี่ยวกับการควบคุมการเข้าถึง โปรดอ่าน ศูนย์ข้อมูลและแกนหลัก ด้านบน สำหรับการกำหนดสิทธิ์ใช้งานและการเข้ารหัสของรหัสผ่าน มีการใช้โปรโตคอล Secure Remote Password (SRP) ซึ่งเป็นโปรโตคอล password-authenticated key agreement (PAKE) เสริม การแทรกซึมหรือการโจมตีผ่านคนกลางจะไม่ได้รับข้อมูลเพียงพอที่จะโจมตีแบบสุ่มรหัสผ่านได้ ซึ่งหมายความว่าสามารถรักษาความปลอดภัยได้อย่างแข็งแกร่งแม้ว่าจะใช้รหัสผ่านที่คาดเดาได้ง่ายก็ตาม
ข้อมูลสำคัญที่อยู่ภายในบัญชี TeamViewer เช่น ข้อมูลการเข้าระบบคลาวด์ จะถูกจัดเก็บโดยเข้ารหัส AES/RSA 2048 บิต

Management Console

TeamViewer Management Console เป็นแพลตฟอร์มบนเว็บสำหรับการจัดการผู้ใช้ การรายงานการเชื่อมต่อและการจัดการคอมพิวเตอร์และผู้ติดต่อ ซึ่งถูกจัดเก็บไว้ในศูนย์ข้อมูลที่เป็นไปตาม HIPAA และได้รับการรับรอง ISO-27001 ข้อมูลทั้งหมดจะถูกถ่ายโอนผ่านช่องทางที่ปลอดภัยด้วยการเข้ารหัส TSL (Transport Security Layer) ซึ่งเป็นมาตรฐานสำหรับการเชื่อมต่อเครือข่ายอินเทอร์เน็ตที่ปลอดภัย นอกจากนี้ ข้อมูลสำคัญจะถูกจัดเก็บโดยเข้ารหัส AES/RSA 2048 บิต สำหรับการกำหนดสิทธิ์ใช้งานและการเข้ารหัสของรหัสผ่าน จะมีการใช้โปรโตคอล Secure Remote Password (SRP) SRP เป็นการกำหนดสิทธิ์ใช้งานตามรหัสผ่านและกระบวนการแลกเปลี่ยนคีย์ที่มีความปลอดภัยและแข็งแกร่งโดยใช้โมดูลัส 2048 บิต

การตั้งค่าตามนโยบาย

ผู้ใช้สามารถกำหนด แจกจ่าย และใช้นโยบายการตั้งค่าสำหรับการติดตั้งซอฟต์แวร์ TeamViewer

บนอุปกรณ์ที่ตัวเองเป็นเจ้าของได้จากภายใน TeamViewer Management Console นโยบายการตั้งค่าจะได้รับการรับรองทางดิจิตอลด้วยบัญชีที่สร้างขึ้นนโยบายนั้นมา
ทั้งนี้เพื่อให้มั่นใจได้ว่ามีเพียงบัญชีที่ได้รับอนุญาตให้กำหนดนโยบายไปยังอุปกรณ์เท่านั้นเป็นบัญชีที่อุปกรณ์นั้นเป็นเจ้าข

ความปลอดภัยของแอปพลิเคชันใน TeamViewer

รายการที่อนุญาตและต้องห้าม

ตัวเลือกเพิ่มเติมด้านการรักษาความปลอดภัยในการจำกัดการเข้าถึงคอมพิวเตอร์ไปยังไคลเอ็นต์ที่เฉพาะเจาะจงจำนวนมาก อาจมีประโยชน์อย่างมากโดยเฉพาะอย่างยิ่งเมื่อใช้ TeamViewer สำหรับการเก็บรักษาคอมพิวเตอร์ที่ไม่มีผู้เฝ้าดู (เช่น ติดตั้ง TeamViewer เป็นบริการของ Windows)

ด้วยฟังก์ชันรายการที่อนุญาต คุณสามารถระบุได้อย่างเฉพาะเจาะจงว่า TeamViewer ID และ/หรือบัญชี TeamViewer ใดที่ได้รับอนุญาตให้เข้าถึงคอมพิวเตอร์ได้ ด้วยฟังก์ชันรายการต้องห้าม คุณสามารถบล็อค TeamViewer ID และบัญชี TeamViewer ที่เฉพาะเจาะจงได้ รายการที่อนุญาตในส่วนกลางเป็นส่วนหนึ่งของ "การตั้งค่าตามนโยบาย" ที่ได้อธิบายไว้ด้านบนในหัวข้อ "Management Console"

การเข้ารหัสแชทและวิดีโอ

ประวัติการแชทเกี่ยวข้องกับบัญชี TeamViewer ของคุณ จึงถูกเข้ารหัสและจัดเก็บไว้โดยใช้การรักษาความปลอดภัยด้วยการเข้ารหัส AES/RSA 2048 บิต ตามที่ได้อธิบายไว้ในหัวข้อ "บัญชี TeamViewer" ข้อความแชทและปริมาณการใช้งานวิดีโอทั้งหมดจะถูกเข้ารหัสอย่างครอบคลุมด้วยการเข้ารหัสเซสชัน AES (256 บิต)

โหมดไม่มีการพรางตัว

ไม่มีฟังก์ชันที่จะทำให้ TeamViewer ทำงานอยู่เบื้องหลังทั้งหมดได้ แม้ว่าแอปพลิเคชันจะทำงานเป็นบริการของ Windows อยู่ในเบื้องหลัง แต่จะมองเห็น TeamViewer ในรูปแบบไอคอนในถาดของระบบเสมอ

หลังจากสร้างการเชื่อมต่อ มักจะมองเห็นแผงควบคุมเล็กๆ ด้านบนถาดของระบบเสมอ TeamViewer จึงได้รับการออกแบบมาให้ไม่เหมาะกับการแอบติดตามคอมพิวเตอร์หรือพนักงาน

การปกป้องรหัสผ่าน

สำหรับการสนับสนุนลูกค้าแบบทันที TeamViewer (TeamViewer QuickSupport) จะสร้างรหัสผ่านเซสชันขึ้นมา (รหัสผ่านแบบครั้งเดียว) หากลูกค้าบอกรหัสผ่านให้กับคุณ คุณก็จะสามารถเชื่อมต่อกับคอมพิวเตอร์ของลูกค้าได้โดยป้อน ID และรหัสผ่านของลูกค้า หลังจากรีสตาร์ท TeamViewer ทางฝั่งลูกค้าแล้ว จะมีการสร้างรหัสผ่านเซสชันใหม่ขึ้นมาเพื่อให้สามารถเชื่อมต่อกับคอมพิวเตอร์ของลูกค้าได้หากได้รับการเชิญเท่านั้น

เมื่อใช้ TeamViewer สำหรับการสนับสนุนระยะไกลที่ไม่มีผู้เฝ้าดู (เช่น ของเซิร์ฟเวอร์) ให้ตั้งรหัสผ่านเฉพาะแบบตายตัวขึ้นมาเพื่อปกป้องการเข้าถึงคอมพิวเตอร์

การควบคุมการเข้าถึงขาเข้าและขาออก

คุณสามารถกำหนดค่าโหมดการเชื่อมต่อ TeamViewer ที่เฉพาะเจาะจงได้ เช่น สามารถกำหนดค่าการสนับสนุนระยะไกลหรือคอมพิวเตอร์ที่ใช้ในการประชุมในรูปแบบที่ไม่สามารถทำการเชื่อมต่อขาเข้าได้

การจำกัดฟังก์ชันการใช้งานของคุณสมบัติที่ต้องการใช้งานจริงๆ เป็นการจำกัดจุดอ่อนสำหรับการโจมตีที่อาจเกิดขึ้น

การรับรองความถูกต้องด้วยสองปัจจัย

TeamViewer ให้ความช่วยเหลือบริษัทต่างๆ ในเรื่องข้อกำหนดในการปฏิบัติตาม HIPAA และ PCI การรับรองความถูกต้องด้วยสองปัจจัยเป็นการเพิ่มชั้นการรักษาความปลอดภัยเพื่อปกป้องบัญชี TeamViewer จากการเข้าถึงที่ไม่ได้รับอนุญาต

นอกจากชื่อผู้ใช้และรหัสผ่านแล้ว ผู้ใช้จะต้องป้อนรหัสเพื่อรับรองความถูกต้อง รหัสนี้จะถูกสร้างขึ้นผ่านอัลกอริทึมรหัสผ่านแบบครั้งเดียว (TOTP) จึงสามารถใช้รหัสได้ในช่วงเวลาสั้นๆ

ด้วยการรับรองความถูกต้องด้วยสองปัจจัยและการจำกัดการเข้าถึงด้วยรายการที่อนุญาต ทำให้ TeamViewer สามารถช่วยสนับสนุนในการปฏิบัติตามหลักเกณฑ์ที่จำเป็นทั้งหมดเพื่อรับการรับรอง HIPAA และ PCI ได้

การทดสอบความปลอดภัย

ทั้งโครงสร้างพื้นฐานของ TeamViewer และซอฟต์แวร์ของ TeamViewer
จะต้องได้รับการทดสอบการโจมตีเป็นประจำ
ซึ่งดำเนินการโดยบริษัทอิสระที่มีความเชี่ยวชาญด้านการทดสอบความปลอดภัย

ต้องการสอบถามเพิ่มเติมหรือไม่

หากต้องการสอบถามหรือขอข้อมูลเพิ่มเติม โปรดติดต่อเราที่ +662 105 5706 หรือส่งอีเมลมาที่ support@teamviewer.com

ติดต่อ

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Germany
service@teamviewer.com