



รักษาความปลอดภัยให้ธุรกิจของคุณ เมื่อจำเป็นต้องทำงานจากระยะไกล

Sebastien Roche ประธานเจ้าหน้าที่ฝ่ายความปลอดภัยข้อมูลของ Alcatel-Lucent Enterprise แบ่งปันข้อมูลเชิงลึกเกี่ยวกับแนวทางของ ALE ในการรักษาความปลอดภัยและความต่อเนื่องทางธุรกิจในช่วงเวลาที่ซับซ้อนนี้

ความเป็นจริงของ#WFH

ด้วยวิกฤตด้านสุขภาพในประเทศต่างๆ ที่เกิดขึ้นไม่นานนี้ และมาตรการให้อยู่แต่ในที่พักอาศัยที่กำหนดขึ้นทั่วโลก ทำให้บริษัทที่ก่อนหน้านี้ ไม่เคยมีตัวเลือกให้ทำงานจากที่บ้าน (#WFH) มาก่อน ต้องเผชิญกับความท้าทายในการเปลี่ยนรูปแบบองค์กร เพื่อรักษาความปลอดภัยและความต่อเนื่องของธุรกิจ

ในปี 2008 ทาง Alcatel-Lucent Enterprise ได้ริเริ่มกลยุทธ์การทำงานจากที่บ้าน ซึ่งได้รับการตอบรับเป็นอย่างดีจากพนักงานมากกว่า 50% จากจำนวน 2,000 คน ที่ทำงานในสำนักงาน 50 แห่งทั่วโลก เมื่อพนักงานของ ALE มากกว่าครึ่งทำงานจากที่บ้าน เราจึงมีเครือข่ายและสถาปัตยกรรมทางเทคโนโลยี สารสนเทศที่จำเป็นต่อการสนับสนุนการทำงานจากระยะไกลอยู่แล้ว ความท้าทายแท้จริงกลับเป็นคำถามที่ว่า เราจะเปลี่ยนจากการมีพนักงานออนไลน์ 50% เป็นพนักงานงานออนไลน์ 100 % ได้อย่างไร

พร้อมสำหรับการดำเนินการ

ในช่วงสามปี ก่อนเกิดวิกฤตด้านการดูแลสุขภาพที่ผ่านมาไม่นานนี้ ALE ได้เริ่มดำเนินการเปลี่ยนแปลงด้านเทคโนโลยี สารสนเทศรอบด้าน โดยมีการนำสถาปัตยกรรมเครือข่าย WAN ที่กำหนดด้วยบริการมาใช้ ซึ่งจะช่วยรักษาความปลอดภัยบนคลาวด์เพื่อสกัดกั้นภัยคุกคามแบบเชิงรุก ระบุหาการโจมตีที่อาจเกิดขึ้น และรับประกันการเข้าถึงที่ปลอดภัยสำหรับพนักงาน

การเปลี่ยนแปลงประกอบด้วยด้านต่างๆ ต่อไปนี้

- การรักษาความปลอดภัยในระบบคลาวด์ด้วยจุดเข้าใช้งานเสมือน
- การติดตามแบบเรียลไทม์
- การระบุรูปแบบพฤติกรรมที่ผิดปกติ เพื่อตรวจหาภัยคุกคาม

โลว์คาร์

รักษาความปลอดภัยให้ธุรกิจของคุณเมื่อจำเป็นต้องทำงานจากระยะไกล





การเตรียมความพร้อม = การตอบสนองที่ ว่องไวในสถานการณ์วิกฤต

มีการตัดสินใจเริ่มทำงานจากระยะไกลในวันจันทร์เมื่อบ่ายวันศุกร์ที่ผ่านมา พนักงานได้รับคำสั่งให้นำแล็ปท็อปและจอภาพกลับบ้านไปด้วย งานในเช้าวันจันทร์เริ่มต้นขึ้นตามปกติโดยไม่มีการหยุดชะงัก ขณะที่พนักงานเริ่มเดินวันใหม่จากห้องทำงานระยะไกลของตนเอง การเปลี่ยนแปลงเครือข่ายที่ดำเนินการไปก่อนหน้านี้ทำให้มั่นใจได้ถึงการเชื่อมต่อระยะไกลที่ปลอดภัยไม่ว่าพนักงานจะอยู่ที่ใด

ความท้าทายในการเข้าถึง

ความท้าทายหลักอย่างหนึ่งที่เราพบคือโปรไฟล์ผู้ใช้ โดยรวมถึงทีมวิจัยและพัฒนา ตลอดจนทีมสนับสนุนด้านเทคนิคที่มีความต้องการเฉพาะในการเข้าถึงเซิร์ฟเวอร์และแพลตฟอร์มการพัฒนาบางประเภทที่โซลูชันการเข้าถึงระยะไกลของเราไม่อนุญาต โปรไฟล์ผู้ใช้ของพนักงานเหล่านี้เข้าใช้งานในโซลูชันการเข้าถึงส่วนตัวที่แตกต่างจากทีมอื่น ๆ

เมื่อเริ่มต้นดำเนินงานเปลี่ยนแปลงเพื่อให้พนักงานทุกคนทำงานแบบ #WFH เราได้ปรับเปลี่ยนโครงสร้างพื้นฐานของเราเพื่อเพิ่มแบนด์วิดท์และเพื่อให้สามารถรองรับการเพิ่มจำนวนการเชื่อมต่อระยะไกลตามความต้องการของพนักงานที่ทำงานจากที่บ้าน

การรักษาความปลอดภัยคือกุญแจสำคัญ

การรักษาความปลอดภัยและการปกป้องข้อมูลขององค์กรมีความสำคัญอย่างยิ่งในช่วงเวลาที่ไม่แน่นอนและยังส่งผลกระทบต่อหลาย ๆ องค์กรที่จัดการกับข้อมูลที่ละเอียดอ่อน เช่น องค์กรภาครัฐ กระทรวง เมืองหลัก และชุมชนเขตเมืองต่าง ๆ

ก่อนที่จะเราเริ่มพูดถึง #WFH กันที่ ALE เราได้นำโครงสร้างพื้นฐานแบบกระจายและมีความปลอดภัยมาใช้งานจริงแล้ว โดยรวมถึงโซลูชันการเชื่อมต่อส่วนตัวที่ใช้ระบบคลาวด์เต็มรูปแบบสำหรับพนักงานทุกคนเพื่อรับประกันความปลอดภัยในการเข้าถึงเครือข่ายจากระยะไกล เรายังคงรักษาโซลูชัน VPN แบบเดิมไว้สำหรับทีมเพียงบางส่วนที่มีความต้องการเฉพาะ เช่น การเชื่อมต่อเครื่องโทรศัพท์ระบบ IP ในห้องทำงานระยะไกลของสมาชิกในทีม นอกจากนี้ เรายังจัดหาคอมพิวเตอร์พีซีระดับมืออาชีพให้พนักงาน ซึ่งมีความสามารถในการจัดการการดาวน์โหลดและการอัปเดตซอฟต์แวร์อัตโนมัติ

ปิดโอกาสในการละเมิดการรักษาความปลอดภัย

ตามที่คาดไว้ ในช่วงเวลาที่มีการทำงานจากระยะไกลกันอย่างแพร่หลายเช่นนี้ การส่งอีเมลการโทรศัพท์เกี่ยวกับอีเมลที่น่าสงสัย และคำขออัปเดตรหัสผ่าน มีจำนวนเพิ่มมากขึ้น ไม่เพียงเท่านั้น การโจมตีแบบฟิชซิง ก็เพิ่มสูงขึ้นอย่างรวดเร็ว เช่นเดียวกับการโจมตีแบบเจาะจงเป้าหมายบนซอฟต์แวร์ที่มีช่องโหว่

แม้ว่าการใช้พริอ็อกซ์ จะปกป้อง ALE จากปัญหาด้านการรักษาความปลอดภัยทางไซเบอร์หลักๆ แต่เรายังคงพบการละเมิดใหม่ๆ ทุกวัน ทั้งจากอีเมลการฉ้อโกง หรือจากการไม่อัปเดตเวอร์ชันของซอฟต์แวร์หรือระบบปฏิบัติการ

เปิดช่องทางการสื่อสารไว้เสมอ

ในช่วงเวลาที่ท้าทายนี้ เรายังคงมีการเชื่อมโยงแบบออนไลน์กับทีม ALE อย่างต่อเนื่อง เราติดต่อสื่อสารกันเป็นประจำ แบ่งปันเคล็ดลับและแนวทางปฏิบัติที่ดีที่สุด แลกเปลี่ยนดูแลให้ทีมของเราพร้อมให้การสนับสนุน แก่พนักงานทุกคน รายการตรวจสอบของ ALE เพื่อการทำงานจากระยะไกลอย่างปลอดภัย

- ไม่อนุญาตหรือสนับสนุนให้ใช้อุปกรณ์ส่วนบุคคล (คอมพิวเตอร์พีซี) ในการแลกเปลี่ยนข้อมูลและการสื่อสารที่เกี่ยวข้องกับการทำงาน
- ดำเนินการให้พนักงานสามารถเข้าถึงได้อย่างเป็นส่วนตัวและปลอดภัย
- ใช้ระบบอัตโนมัติในการอัปเดตซอฟต์แวร์ทั่วทั้งเครือข่ายองค์กร
- ใส่ใจกับคำขอทางอีเมลที่น่าสงสัย
- ใช้ซอฟต์แวร์ที่ผ่านการรับรองแล้ว การตรวจสอบและการรับรองจะช่วยพิสูจน์ยืนยันความน่าเชื่อถือในการรักษาความปลอดภัยของซอฟต์แวร์
- ลดความซับซ้อนของกระบวนการตัดสินใจ ในสถานการณ์ฉุกเฉิน CISO หรือ CIO จำเป็นต้องตัดสินใจอย่างรวดเร็ว เพื่อแก้ไขปัญหาให้บริการมีความต่อเนื่อง

ใบข่าว

รักษาความปลอดภัยให้ธุรกิจของคุณเมื่อจำเป็นต้องทำงานจากระยะไกล



คำแนะนำนำหกรจาก ALE เพื่อการเชื่อมต่อนะยะไกลที่ปลอดภัย



1. ใช้ระบบอัตโนมัติเพื่อแจ้งเตือนการเปลี่ยนรหัสผ่าน

ช่วยพนักงานเปลี่ยนรหัสผ่านขององค์กรก่อนที่จะหมดอายุ ก่อนวันหมดอายุ พนักงานจะได้รับอีเมลประจำวันพร้อมคำแนะนำให้พนักงานเปลี่ยนรหัสผ่าน

2. เปิดใช้งานการสำรองข้อมูลในระบบคลาวด์

อนุญาตและสนับสนุนให้พนักงานบันทึกข้อมูลของตนเองเป็นประจำเพื่อหลีกเลี่ยงการสูญเสียข้อมูล ในกรณีที่แล็ปท็อปมีปัญหา เปิดใช้งานพื้นที่เก็บข้อมูลสำรอง และให้ความช่วยเหลือระยะไกลผ่านฝ่ายให้บริการช่วยเหลือทางเทคโนโลยีสารสนเทศหรือผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศตามความจำเป็น

3. เตือนให้พนักงานทราบถึงแนวทางปฏิบัติที่ดีที่สุด ในการปกป้องอุปกรณ์

ดูแลแล็ปท็อปของคุณให้อยู่ในสภาพดีเยี่ยมโดยปฏิบัติตามนี้

- ปิดแล็ปท็อปเมื่อใช้งานเสร็จในแต่ละวัน (หลีกเลี่ยงโหมดสลีป/โหมดล็อค)
- เก็บแล็ปท็อปให้ห่างจากแหล่งให้ความร้อน (เช่น แสงแดด หรือเครื่องทำความร้อน)
- หลีกเลี่ยงการรับประทานอาหารหรือดื่มเครื่องดื่มใกล้กับแล็ปท็อป
- เก็บสายเคเบิลไว้ให้ห่างจากเด็กและสัตว์เลี้ยง

4. คำนิ้งถึงการรักษาความปลอดภัยเป็นอันดับแรก

ให้ความรู้ แก่ทีมเกี่ยวกับความเสี่ยงและแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัย

- กระตุ้นให้พนักงานคิดทบทวนก่อนที่จะคลิกลิงค์ ถึงแม้จะดูเหมือนว่าส่งมาจากบุคคลที่คุ้นเคยก็ตาม
- ให้พนักงานสามารถติดตามผลกับฝ่ายเทคโนโลยีสารสนเทศได้ ในกรณีที่มีข้อสงสัย

- จัดเตรียมเครื่องมือสำหรับการรายงานอีเมลที่น่าสงสัย
- นำแนวทางการเล่นเกมสมาธิประยุกต์ใช้ (Gamification) ในการสร้างวัฒนธรรมที่ให้ความสำคัญกับการรักษาความปลอดภัยเป็นอันดับแรก โดย ALE ใช้วิธีนี้ เพื่อส่งเสริมให้พนักงานตรวจหาและรายงานอีเมลที่น่าสงสัย

5. ติดต่อสื่อสาร

ความโดดเด่นทำให้ผู้คนเสี่ยงต่อการถูกโจมตีทางไซเบอร์ ค้นหาวีธีที่ทำให้ทีมของคุณเชื่อมโยงถึงกัน

- จัดให้มีการแลกเปลี่ยนข้อมูลข่าวสารเป็นประจำ รวมถึงการประชุมออนไลน์ กิจกรรมพื้นที่ ที่ทำงานร่วมกันและงานสังสรรค์
- ส่งเสริมให้พนักงานติดต่อกับทีมของตนอย่างสม่ำเสมอ
- ส่งอีเมลเป็นประจำเพื่อแจ้งให้พนักงานทราบว่า ทีมเทคโนโลยีสารสนเทศพร้อมให้ความช่วยเหลือ และเตือนพนักงานให้ทราบถึงแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยอย่างสม่ำเสมอ

6. ส่งเสริมอุปนิสัยด้านการเชื่อมต่อที่ดี

ความเสี่ยงในการทำงานจากระยะไกลคือ การทำงาน 12 ชั่วโมงต่อวัน โดยมีการเชื่อมต่ออย่างต่อเนื่องหรือการประชุมติดต่อกันยาวนาน ส่งเสริมให้พนักงานมีเวลาพักจากหน้าจอและตัดขาดการติดต่อสื่อสารนอกเวลาทำงานได้ แล้วใช้เวลากับครอบครัวหรือทำกิจกรรมนอกบ้าน

Alcatel-Lucent Rainbow สำหรับการร่วมมือทำงานที่เชื่อมโยงถึงกัน

Rainbow แพลตฟอร์มการทำงานร่วมกันบนคลาวด์สำหรับการแชท การสนทนาทางวิดีโอ และเสียง รวมถึงการแชร์หน้าจอและเอกสาร ช่วยให้พนักงานของ ALE มีเครื่องมือที่ตนต้องการ เพื่อให้ยังคงเชื่อมโยงถึงกัน ในเวลา #WFH เช่นนี้ พนักงานทุกคนใช้แพลตฟอร์มดังกล่าว กันอย่างกว้างขวางในการทำงานร่วมกับเพื่อนร่วมงาน

นอกจากนี้ พันธมิตรและลูกค้าของเรายังเลือกใช้ Rainbow โดยให้เป็นโซลูชันการทำงานร่วมกัน ที่ตรงใจที่สุด Rainbow ตอบสนองความต้องการด้านการรักษาความปลอดภัยของภาครัฐ การป้องกันประเทศ การดูแลสุขภาพ และภาคส่วนเฉพาะอื่นๆ ทั้งยังสอดคล้องกับกฎระเบียบด้านการรักษาความปลอดภัย



โทรศัพท์

รักษาความปลอดภัยให้ธุรกิจของคุณเมื่อจำเป็นต้องทำงานจากระยะไกล



สนับสนุนชุมชนของเรา

จากการดำเนินงานในแคมเปญความต่อเนื่องทางธุรกิจ ALE ได้ให้สิทธิ์โดยไม่คิดค่าใช้จ่าย เพื่อช่วยสนับสนุนองค์กร เมือง และรัฐบาล ในการรักษาความต่อเนื่องของบริการ นอกจากนี้ เราได้ขยายขีดความสามารถในการโฮสต์บนคลาวด์ของเรา เพื่อตอบสนองความต้องการรวมถึงจำนวนผู้ใช้ที่พุ่งสูงขึ้นอีกด้วย หากต้องการทราบข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยทางไซเบอร์ โปรดดูคำแนะนำจากหน่วยงานด้านการรักษาความปลอดภัยทางไซเบอร์ของสหภาพยุโรป

www.al-enterprise.com ชื่อและโลโก้ Alcatel-Lucent เป็นเครื่องหมายการค้าของ Nokia ซึ่ง ALE ใช้ภายใต้สิทธิ์การใช้งาน หากต้องการดูเครื่องหมายการค้าอื่น ๆ ที่ใช้โดยบริษัทในเครือของ ALE Holding ให้ไปที่ www.al-enterprise.com/en/legal/trademarks-copyright เครื่องหมายการค้าอื่น ๆ ทั้งหมดเป็นทรัพย์สินของเจ้าของที่เกี่ยวข้อง ข้อมูลที่นำเสนออาจมีการเปลี่ยนแปลงโดยไม่ต้องแจ้งให้ทราบล่วงหน้า ทั้ง ALE Holding และบริษัทในเครือจะไม่รับผิดชอบต่อความไม่ถูกต้องภายในเอกสารฉบับนี้ © Copyright 2023 ALE International, ALE USA Inc. สงวนลิขสิทธิ์ในทุกประเทศ DID20060201TH (อาจ 2023)