เอกสารให้ความรู้ด้านความปลอดภัยไซเบอร์-ศบส.10

ทำไมธุรกิจขนาดเล็กถึงถูกโจมตีบ่อยกว่าธุรกิจขนาดใหญ่?

การโจมตีทางไซเบอร์ส่วนใหญ่นั้นใช้เพื่อเก็บข้อมูลส่วนบุคคลที่ใช้ในบัตรเครดิตหรือการโจรกรรมระบุตัวตน ในขณะที่องค์กรขนาดใหญ่โดยทั่วไปมีข้อมูลที่จะขโมยได้มากกว่า ธุรกิจขนาดเล็กกว่าก็มีเครือข่ายที่ปลอดภัยน้อยกว่า ทำให้ง่ายต่อการละเมิดในการเข้าถึงเครือข่าย

ธุรกิจของคุณจะหลีกเลี่ยงการตกเป็นเหยื่อของการโจมตีทางไซเบอร์ได้อย่างไร?

นี่คือแนวทางปฏิบัติที่ดีที่สุดด้านการรักษาความปลอดภัยสารสนเทศและโลกไซเบอร์สำหรับธุรกิจ ทักษะด้านความปลอดภัยในโลกไซเบอร์ ที่องค์กรธุรกิจของคุณควรจะมี สามารถเริ่มนำไปใช้ได้วันนี้:

1. ใช้ไฟร์วอลล์
2. กำหนดเอกสารนโยบายความปลอดภัยทางไซเบอร์ของคุณ
3. บังคับใช้รหัสผ่านที่ปลอดภัย
4. ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์
5. มีความตระหนักถึงสื่อสังคม
6. ระมัดระวังในการซอฟต์แวร์ฟรี
7. แบ่งระบบเครือข่ายของคุณ
8. ให้ความรู้แก่พนักงานทุกคน
9. สำรองข้อมูลทั้งหมดเป็นประจำ
10. ใช้การระบุตัวตนแบบหลายปัจจัย
11. ใช้การเข้ารหัส และแบ่งแยกข้อมูลลูกค้า
12. เพิ่มความปลอดภัยให้กับอีเมลของคุณ

แนวทางปฏิบัติด้านความปลอดภัยที่ดีที่สุด สำหรับบริษัทขนาดเล็กที่มีพนักงานสูงสุด 20-50 คน

1. ใช้ไฟร์วอลล์

หนึ่งในแนวป้องกันแรกในการโจมตีทางไซเบอร์คือไฟร์วอลล์ ถึงธุรกิจขนาดเล็กก็ควรตั้งค่าไฟร์วอลล์เพื่อให้เป็นอุปสรรคระหว่างข้อมูลและอาชญากรไซเบอร์ของคุณนอกเหนือจากไฟร์วอลล์ภายนอกที่มาตรฐานแล้ว หลายบริษัทกำลังเริ่มติดตั้งไฟร์วอลล์ภายในเพื่อให้มีการเพิ่มเติมระบบป้องกันการโจมตีบนโลกไซเบอร์สิ่งสำคัญคือพนักงานที่ทำงานจากที่บ้าน ได้ติดตั้งไฟร์วอลล์บนเครือข่ายภายในบ้านของพวกเขาเช่นกัน พิจารณาจัดหาซอฟต์แวร์ไฟร์วอลล์ และสนับสนุนเครือข่ายภายในบ้านเพื่อให้แน่ใจว่าสอดคล้องกัน

2. แบ่งระบบเครือข่ายของคุณ

วิธีในการปกป้องเครือข่ายของคุณคือการแยกเครือข่ายของคุณออกเป็นโซน และป้องกันโซนอย่างเหมาะสม โซนหนึ่งอาจใช้สำหรับงานที่สำคัญเท่านั้น ซึ่งโซนอื่นอาจเป็นโซนเพื่อผู้เยี่ยมชมที่ลูกค้าสามารถเข้ามาจากการท่องอินเทอร์เน็ต แต่ไม่สามารถเข้าถึงเครือข่ายที่ทำงานของคุณได้

แบ่งเครือข่ายของคุณ และตั้งข้อกำหนดด้านความปลอดภัยที่เข้มงวดมากขึ้น ในกรณีที่จำเป็น

- เว็บเซิร์ฟเวอร์สาธารณะ ไม่ควรได้รับอนุญาตให้เข้าถึงเครือข่ายภายในของคุณ
- คุณอาจอนุญาตการเข้าถึงในแบบผู้เยี่ยมชม แต่ไม่อนุญาตให้ผู้นั้นมาอยู่ในเครือข่ายภายในของคุณ
- พิจารณาแยกเครือข่ายของคุณ ตามหน้าที่ของธุรกิจต่างๆ (ส่วนบันทึกลูกค้า การเงิน พนักงานทั่วไป)

3. กำหนดเอกสารนโยบายความปลอดภัยทางไซเบอร์ของคุณ

ในขณะที่ธุรกิจขนาดเล็กมักดำเนินงานด้วยคำพูดจากปากและความรู้ที่ชาญฉการป้องกันภัยคุกคามและการรักษาความปลอดภัยบนโลกไซเบอร์เป็นหนึ่งในบริเวณที่จำเป็นต่อการจัดทำเอกสารแบบพิธีของคุณ

นโยบายดังกล่าวควรแจ้งให้พนักงานของคุณ และผู้ที่ได้รับการอนุมัติในการรับผิดชอบของพวกเขา เพื่อปกป้องเทคโนโลยีและข้อมูลสินทรัพย์ของธุรกิจของคุณ บางประเด็นที่นโยบายควรครอบคลุมคือ:

- ประเภทของข้อมูลธุรกิจที่สามารถแบ่งปันได้ และแห่งใดบ้าง
- การใช้อุปกรณ์และการสื่อออนไลน์ ที่สามารถยอมรับได้
- การจัดการและการเก็บรักษาเนื้อหาที่มีตวามละเอียดอ่อนและสำคัญ

ธุรกิจที่ไม่มีนโยบายความปลอดภัยในโลกไซเบอร์ อาจเปิดโอกาสให้ตัวเองถูกโจมตีและปัญหาทางกฎหมาย

4. ให้ความรู้แก่พนักงานทุกคน

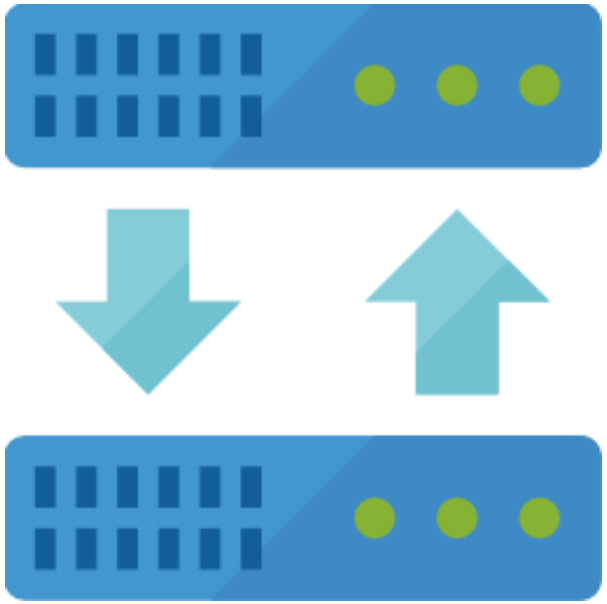
พนักงานมักจะสวมหมวกหลายใบ (คุณไม่มีทางรู้ว่าใครจะไว้ใจได้) ในบริษัทขนาดเล็ก ทำให้มันเป็นเรื่องจำเป็นที่พนักงานทุกคนที่เข้าถึงเครือข่าย ต้องได้รับการฝึกอบรมเกี่ยวกับแนวทางปฏิบัติที่ดีที่สุดด้านความปลอดภัยในโลกไซเบอร์ และการป้องกันภัยคุกคามทางคอมพิวเตอร์

เนื่องจากนโยบายต้องมีการพัฒนา เมื่ออาชญากรไซเบอร์กลายเป็นคนที่ฉลาดกว่า จึงจำเป็นต้องมีการอัปเดตโปรโตคอลใหม่เป็นประจำ ก้าวทันภัยคุกคามด้านไอที เพื่อให้พนักงานทุกคนมีความรับผิดชอบ ควรให้พนักงานแต่ละคนลงนามในเอกสารเพื่อระบุว่าพวกเขาได้รับแจ้งเกี่ยวกับนโยบายและเข้าใจว่าอาจมีการดำเนินการ หากไม่ปฏิบัติตามนโยบายด้านความปลอดภัย

5. บังคับใช้รหัสผ่านที่ปลอดภัย

ใช่ พนักงานพบว่าการเปลี่ยนรหัสผ่านเป็นสิ่งที่เจ็บปวด อย่างไรก็ตามรายงานการตรวจสอบการละเมิดข้อมูลของ Verizon ปี 2016 พบว่า 63 เปอร์เซ็นต์ของการละเมิดข้อมูลเกิดขึ้น เนื่องจากรหัสผ่านที่เกิดสูญหาย ถูกขโมย หรืออ่อนแอ

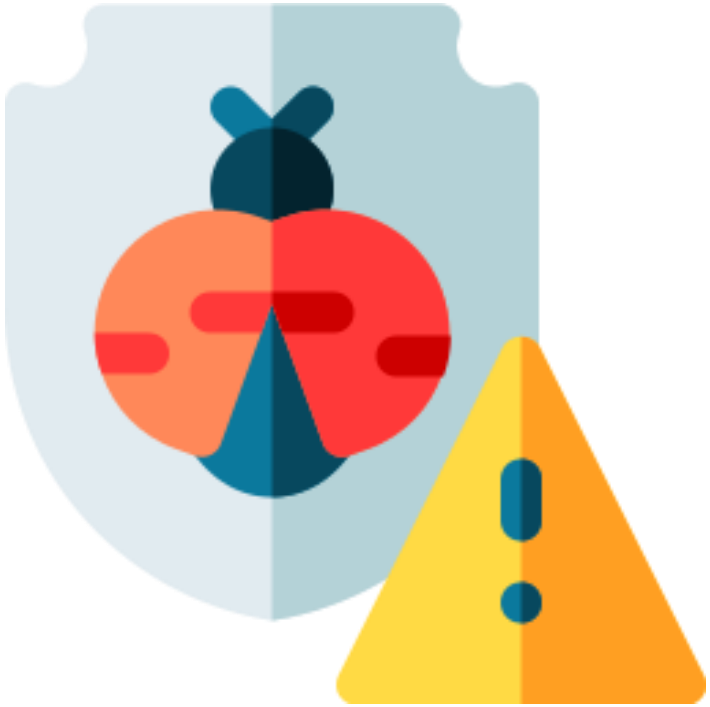
ร้อยละ 65 ของธุรกิจขนาดเล็ก ไม่ได้บังคับใช้นโยบายของรหัสผ่าน ในโลกของ BYOD (นำอุปกรณ์ของคุณมาเอง) ในวันนี้ จำเป็นอย่างยิ่งที่อุปกรณ์ของพนักงานทุกคน ที่เข้าถึงเครือข่ายของบริษัท จะได้รับการป้องกันด้วยรหัสผ่าน



6. สำรองข้อมูลทั้งหมดเป็นประจำ

แม้ว่าจะเป็นสิ่งสำคัญที่จะต้องป้องกันการโจมตีให้ได้มากที่สุด แต่ก็ยังสามารถถูกละเมิดได้โดยไม่คำนึงถึงการระมัดระวังของคุณ ให้สำรองข้อมูล เอกสารประมวลผลคำ สเปรดชีต อิเล็กทรอนิกส์ ฐานข้อมูล ไฟล์การเงิน ไฟล์ทรัพยากรมนุษย์ และไฟล์ลูกหนี้ / เจ้าหนี้

อย่าลืมสำรองข้อมูลทั้งหมดให้เก็บไว้บนคลาวด์ด้วย
ตรวจสอบให้แน่ใจว่าการสำรองข้อมูลถูกเก็บไว้ในตำแหน่งที่แยกต่างหาก ในกรณีเกิดอัคคีภัยหรือน้ำท่วม เพื่อให้แน่ใจว่าคุณจะมีข้อมูลสำรองล่าสุด หากคุณต้องการ ให้ตรวจสอบข้อมูลสำรองของคุณเป็นประจำ เพื่อให้แน่ใจว่าข้อมูลนั้นทำงานได้อย่างถูกต้อง



7. ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์

เป็นการง่ายที่จะสมมติว่าพนักงานของคุณรู้ว่าจะไม่เคยเปิดอีเมลฟิชชิง อย่างไรก็ตาม รายงานการตรวจสอบการละเมิดข้อมูลของ Bitdefender Data Breach Investigations Report พบว่าผู้ใช้มากกว่า 30 เปอร์เซ็นต์เปิดอีเมลฟิชชิงและมีจำนวนเพิ่มขึ้นทุกปี เนื่องจากการโจมตีแบบฟิชชิงเกี่ยวข้องกับการติดตั้งมัลแวร์ในคอมพิวเตอร์ของพนักงาน เมื่อมีการคลิกลิงก์ จึงจำเป็นต้องมีซอฟต์แวร์ป้องกันมัลแวร์ติดตั้งในทุกอุปกรณ์และเครือข่าย การโจมตีด้วยฟิชชิงมักจะมุ่งไปที่บทบาทของพนักงานโดยเฉพาะธุรกิจขนาดเล็ก และใช้กลยุทธ์เฉพาะตำแหน่งเช่น:

- ผู้บริหารระดับสูง
- ผู้ช่วยฝ่ายบริหาร
- พนักงานขาย
- ทรัพยากรมนุษย์

8. ใช้การระบุตัวตนแบบหลายปัจจัย

ไม่ว่าคุณจะเตรียมการอย่างไร พนักงานอาจทำผิดพลาดด้านความปลอดภัย ซึ่งอาจทำให้ข้อมูลของคุณไม่ปลอดภัย Matt Littleton ผู้อำนวยการภูมิภาค Cybersecurity และ Azure Infrastructure Services ของ Microsoft กล่าวว่าการใช้การตั้งค่าการระบุตัวตนแบบหลายปัจจัยในเครือข่ายหลัก และผลิตภัณฑ์อีเมล ส่วนใหญ่นั้นทำได้ง่ายและให้การปกป้องอีกชั้นหนึ่ง เขาแนะนำให้ใช้หมายเลขโทรศัพท์ของพนักงานเป็นรูปแบบที่สอง เนื่องจากเป็นไปได้ยากที่โจรจะมีทั้งรหัส PIN และรหัสผ่าน

ความปลอดภัยเป็นเป้าหมายเคลื่อนที่ อาชญากรไซเบอร์ก้าวหน้าขึ้นไปทุกวัน เพื่อปกป้องข้อมูลของคุณให้ได้มากที่สุด สิ่งสำคัญคือพนักงานทุกคนต้องให้ความสำคัญกับความปลอดภัยทางไซเบอร์เป็นอันดับแรก และที่สำคัญที่สุดคือคุณยังคงอยู่บนแนวโน้มที่ล่าสุดสำหรับการโจมตี และเทคโนโลยีการป้องกันใหม่ล่าสุด โดยธุรกิจของคุณขึ้นอยู่กับมัน

9. มีความตระหนักถึงสื่อสังคม

เว็บไซต์โซเชียลมีเดียนั้นเป็นสิ่งที่อยู่ในใจ สำหรับอาชญากรไซเบอร์ ที่ต้องการรับผลประโยชน์ข้อมูลเกี่ยวกับผู้คนเพื่อปรับปรุงอัตราความสำเร็จในการโจมตี เช่น ฟิชชิ่ง สเปียร์ฟิช หรือวิศวกรรมทางสังคม เริ่มต้นด้วยการรวบรวมข้อมูลส่วนบุคคล ของแต่ละรายบุคคล

- ให้ความรู้แก่พนักงาน ให้ระมัดระวังในการแบ่งปันบนเว็บไซต์ โซเชียลมีเดีย แม้ในบัญชีส่วนตัวของพวกเขา
- แจ้งให้ผู้ใช้ทราบว่าอาชญากรไซเบอร์จะสร้างโปรไฟล์ของพนักงานบริษัท เพื่อให้การโจมตีแบบฟิชชิ่งและวิศวกรรมทางสังคมประสบความสำเร็จมากขึ้น
- อบรมพนักงานเกี่ยวกับการตั้งค่าความเป็นส่วนตัวในเว็บไซต์โซเชียลมีเดีย เพื่อปกป้องข้อมูลส่วนบุคคลของพวกเขา
- ผู้ใช้ควรระมัดระวังสิ่งที่พวกเขาแบ่งปัน เนื่องจากอาชญากรไซเบอร์สามารถเดาคำตอบเพื่อความปลอดภัย (เช่นชื่อสุนัขของคุณ) เพื่อรีเซ็ตรหัสผ่านและเข้าถึงบัญชี

10. ใช้การเข้ารหัส และแบ่งแยกข้อมูลลูกค้า

ธุรกรรมออนไลน์สร้างขึ้นจากความเชื่อมั่นของลูกค้า หลังจากนั้นพวกเขามักใส่เงินจำนวนมากเข้าบัญชีของคุณ ด้วยความเชื่อที่ว่าคุณจะคงอยู่จนถึงสิ้นการต่อรอง
ความไว้วางใจนั้นเป็นทรัพย์สินที่สำคัญที่สุดของคุณ
ดังนั้นเมื่อคุณได้จัดเก็บข้อมูลลูกค้าทางออนไลน์ ให้เข้ารหัสข้อมูลและจัดเก็บองค์ประกอบที่แตกต่างกันในสถานที่ที่แตกต่างกัน เพื่อให้การละเมิดความปลอดภัยอย่างใดอย่างหนึ่ง ไม่ให้นำฐานข้อมูลทั้งหมดออกไป

11. ระมัดระวังในการซอฟต์แวร์ฟรี

พวกเราหลายคนมีแอพจำนวนมากบนโทรศัพท์มือถือของเรา และเราไม่ได้จ่ายเงินใด ๆ เลือกซอฟต์แวร์ที่น่าเชื่อถือ และตรวจสอบได้ดี
คุณอาจไม่ทราบ แต่ซอฟต์แวร์อาจมาพร้อมกับโทรจันที่ซ่อนอยู่ ซึ่งสามารถขโมยข้อมูล รหัสผ่าน และข้อมูลประจำตัวของคุณได้

12. เพิ่มความปลอดภัยให้กับอีเมลของคุณ

เกือบครึ่งหนึ่งของไฟล์แนบอีเมลที่เป็นอันตรายทั้งหมด มาจากไฟล์ office

ข้อควรระวังความปลอดภัยขั้นพื้นฐานของอีเมล เช่น ไม่เปิดไฟล์แนบ หรือลิงก์ที่น่าสงสัย เป็นขั้นตอนแรกที่สามารถกล่าวถึงในแผนการฝึกอบรมพนักงานของคุณ หากคุณต้องจัดการกับข้อมูลส่วนบุคคลของลูกค้า คุณสามารถเข้ารหัสเอกสารเพื่อให้ทั้งผู้ส่งและผู้รับ ต้องใช้รหัสผ่านเพื่อเปิด

วิธีการเริ่มต้น

เมื่ออินเทอร์เน็ตเข้าถึงได้ง่ายขึ้น และเราได้แบ่งปัน รวบรวมข้อมูล รวมถึงข้อมูลทางออนไลน์เพิ่มเติม คุณต้องมั่นใจว่ามีมาตรกาการป้องกันภัยไอที ของโครงสร้างพื้นฐานสำคัญสำหรับธุรกิจจำนวนมาก สิ่งนี้รวมถึงข้อมูลของธุรกิจที่คุณได้สร้างและจัดเก็บ รวมถึงข้อมูลของลูกค้าที่ได้แบ่งปันของคุณ การให้การตั้งค่าที่ปลอดภัยนั้นเป็นสิ่งสำคัญในการสร้างและรักษาความเชื่อมั่น และไว้วางใจในธุรกิจของคุณ

แผนกไอทีของคุณจะต้องสามารถค้นหาและควบคุมปัญหาได้อย่างรวดเร็ว การฝ่าฝืนละเมิดที่เกิดขึ้น หยุดยั้งภัยคุกคามด้านความปลอดภัยทางไซเบอร์จากภายในธุรกิจ ขั้นตอนในรายการตรวจสอบนี้จะลดโอกาสที่เกิดขึ้น แต่ไม่มีการป้องกันความปลอดภัยใด ๆ ที่จะสามารถป้องกันได้อย่างสมบูรณ์

คุณต้องมีระบบและกลยุทธ์เพื่อค้นหา และควบคุมปัญหาอย่างทั่วทั้งบริษัทของคุณ

Cr. https://www.bitdefender.co.th/