10 ภัยคุกคามความปลอดภัยทางไซเบอร์ในปี 2020 ที่มีแนวโน้มเพิ่มขึ้น

สำหรับปี 2020 จะเห็นได้ว่าในช่วงที่ผ่านมา พบข่าวมัลแวร์และภัยคุกคามไซเบอร์หลากหลายประเภท ซึ่งตรงกับที่คาดการณ์ไว้ในบทความ Cybersecurity Prediction 2020 และคาดการณ์ว่าจะพบภัยคุกคามเพิ่มขึ้นอีก ซึ่งทุกองค์กรต้องเตรียมรับมือ เตรียมความพร้อมทีมงานเฉพาะด้าน Cybersecurity เพราะไม่อาจรู้ว่าจะเกิดภัยคุกคามประเภทใดกับองค์กรในอนาคต และบทความนี้จะบอกถึงการคาดการณ์จากผู้เชี่ยวชาญทางด้าน Cybersecurity ว่า 10 อันดับภัยคุกคามที่จะเกิดขึ้นในปี 2020 ที่มีแนวโน้มเพิ่มสูงขึ้น และจะวิธีการป้องกันระบบไอทีของเราเบื้องต้นอย่างไรให้ปลอดภัย

1. การโจมตีแบบฟิชชิง (Phishing Attacks)

โดยทั่วไปการหลอกลวงแบบฟิชชิงจะใช้วิศวกรรมทางสังคม (Social Engineer) เพื่อขโมยข้อมูลของผู้ใช้งาน และการโจมตีบริการคลาวด์ โดยพบว่าเกือบร้อยละ 78 ของเหตุการณ์จารกรรมทางไซเบอร์ในปี 2019 พบว่าเกี่ยวข้องกับฟิชชิง และมีแนวโน้มที่เพิ่มขึ้นในปี 2020

ซึ่งในปี 2020 การใช้คลาวด์เพิ่มมากขึ้นและเป็นไปได้สูงว่าจะพบการทำฟิชชิงผ่านแอปพลิเคชันบนคลาวด์ ด้วยการที่บริการคลาวด์มีระบบรักษาความปลอดภัยขั้นพื้นฐานอยู่แล้ว จึงทำให้ผู้ใช้งานไว้วางใจระบบและแอปพลิเคชันต่าง ๆ จนอาจประมาทเลินเล่อ ไม่ได้ระมัดระวังอย่างเต็มที่ ก็อาจถูกภัยฟิชชิงแบบไม่ตั้งใจได้

2. การรักษาความปลอดภัยของผู้ปฏิบัติงานด้วยการ Remote

ในการทำงานโดยใช้ Remote มักจะทำงานโดยไม่มีการรักษาความปลอดภัย เพราะการทำงานทางไกลบางครั้ง เครือข่าย สัญญาณอินเทอร์เน็ตสาธารณะไม่มีการรักษาความปลอดภัยที่ดี และอุปกรณ์มือถือบางยี่ห้อมักจะสามารถปกปิดสัญญาณที่บ่งบอกถึงการโจมตีแบบฟิชชิ่ง และภัยคุกคามความปลอดภัยทางไซเบอร์อื่น ๆ ได้ ซึ่งผู้เชี่ยวชาญด้านความปลอดภัยของ WatchGuard คาดการณ์ว่าในปี 2020 ร้อยละ 25 จะพบการรั่วไหลของข้อมูลทั้งหมดจะเกี่ยวข้องกับสินทรัพย์ภายนอกองค์กร อย่างอุปกรณ์มือถือ และผู้ให้บริการด้านโทรคมนาคมอย่างแน่นอน

/3. การหลอกลวง...

3. การหลอกลวงบนคลาวด์ (Cloud Jacking)

Cloud Jacking มีแนวโน้มว่าจะเป็นหนึ่งในภัยคุกคามทางไซเบอร์ที่โดดเด่นที่สุดในปี 2020 เนื่องจากการเพิ่มขึ้นของการพึ่งพาธุรกิจบนคลาวด์ หากมีการกำหนดค่าที่ผิดพลาดจะทำให้เหตุการณ์การโจมตีส่วนใหญ่เป็นไปตามรายงานของ Sophos 2020 Threat Report

Trend Micro คาดการณ์ว่าการโจมตีด้วยการ Injection Attacks ไม่ว่าโดยตรง หรือผ่าน Third-party Library จะถูกใช้อย่างเด่นชัดกับแพลตฟอร์มคลาวด์ การโจมตีเหล่านี้จากการเขียนสคริปต์ข้ามไซต์และการทำ SQL Injection จะทำการดักฟังควบคุมและแม้แต่แก้ไขไฟล์และข้อมูลสำคัญที่เก็บไว้ในคลาวด์ ผู้โจมตีจะทำการ Injection Attacks ที่เป็นอันตรายไปยัง Third-Party Library ซึ่งผู้ใช้งานจะดาวน์โหลดและนำมาใช้งานโดยไม่ตั้งใจ

ดังที่ระบุไว้ใน บล็อก 2020 Predictions and Trends ของ Cybersecurity Forcepoint ผู้ขายคลาวด์สาธารณะทั่วไปที่มีความรับผิดชอบร่วมกันระบุว่า ผู้ให้บริการคลาวด์มีหน้าที่รับผิดชอบในการปกป้องโครงสร้างพื้นฐานในขณะที่ลูกค้าจะรับผิดชอบในการปกป้องข้อมูลของพวกเขา ช่องโหว่ของระบบและการแก้ไขต่างๆ ดังนั้นความรับผิดชอบด้านความปลอดภัยจำนวนมากจึงขึ้นอยู่กับความรับผิดชอบของลูกค้านั่นเอง

4. อุปกรณ์ IoT

รายงานจาก Fortune Business ระบุว่า Internet of Things (IoT) มีแนวโน้มที่จะเติบโตถึง 1.1 ล้านล้านดอลลาร์ ภายในปี 2026 โดยไม่จำเป็นต้องพูดว่าการใช้งานอุปกรณ์ IoT ที่แพร่หลายนี้จะช่วยเตือนภัยเรื่องการคุกคามความปลอดภัยทางไซเบอร์ที่ซับซ้อนมากขึ้น นอกจากนี้ยังอาจมีภัยคุกคามร้ายแรงต่อ Internet of Medical Things (IoMT) ที่อาจกลายเป็นวิกฤตสุขภาพที่ร้ายแรง

ความจริงที่ว่าอุปกรณ์ IoT ใหม่ส่วนใหญ่ยังอยู่ในช่วงเริ่มต้นหมายความว่ามีพื้นที่การโจมตีที่ใหญ่กว่ามากสำหรับอาชญากรไซเบอร์เพื่อกำหนดเป้าหมายช่องโหว่ที่เกี่ยวข้องกับเทคโนโลยีใหม่ๆ นอกจากนี้ยังเป็นเรื่องยากที่จะพัฒนากลยุทธ์ความปลอดภัยทางไซเบอร์เพื่อให้ทันกับการเกิดขึ้นอย่างรวดเร็วของอุปกรณ์ IoT ใหม่ๆ

5. การโจมตี Ransomware ที่ซับซ้อนและตรงเป้าหมาย

Ransomware การโจมตีเป็นปัญหาสำคัญสำหรับธุรกิจในช่วงสองสามปีที่ผ่านมา เหตุผลที่ Ransomware มีมานานแล้วก็คือหาใช้งานได้ง่าย ซึ่งผู้ถูกโจมตีจะได้รับผลกระทบร้ายแรง สามารถหาได้ในราคาถูกและพร้อมใช้งานบน Dark web

ในปี 2020 เราอาจเห็นการเกิดขึ้นของการโจมตี ransomware ที่ซับซ้อนและมีเป้าหมาย กลุ่มการสอบสวนทางไซเบอร์ที่ McAfee, John Fokker คาดการณ์ว่า ransomware มีแนวโน้มที่จะรวมเข้ากับมิจฉาชีพทำให้เกิดการสร้างตระกูลมัลแวร์ as-a-service น้อยลง แต่มีประสิทธิภาพมากขึ้นซึ่งจะทำงานร่วมกับคนอื่น

กลุ่มการสอบสวนทางไซเบอร์ยังกล่าวเพิ่มเติมว่า จะมีการสานต่อแบรนด์ ransomware ที่ทรงพลังที่สุดซึ่งใช้โครงสร้างพันธมิตรเพื่อทำให้ภัยคุกคามของพวกเขารุนแรงยิ่งขึ้น นี่เป็นสาเหตุสำคัญของความกังวลเนื่องจากผลกระทบจากการโจมตีเพียงครั้งเดียวของ ransomware ก็สามารถสร้างความเสียหายอย่างมากให้กับธุรกิจขนาดเล็กและขนาดกลางนำไปสู่ต้นทุนที่สูงขึ้นเนื่องจากการหยุดทำงาน และการกู้คืนระบบ

/6. การปลอมแปลง...

6. การปลอมแปลง (Deepfakes)

Deepfake คือการใช้การเรียนรู้ของเครื่องและปัญญาประดิษฐ์ (AI) เพื่อจัดการภาพหรือวิดีโอที่มีอยู่ของบุคคลเพื่อแสดงกิจกรรมบางอย่างที่ไม่ได้เกิดขึ้นจริง มีการคาดการณ์ว่าที่ในที่สุด Deepfakes อาจจะปรากฏว่าเป็นภัยคุกคามทางไซเบอร์ที่สำคัญโดยมีการใช้เพื่อจุดประสงค์ที่เลวร้าย

มีความเป็นไปได้ที่จะใช้เทคนิค Deepfake ในความพยายามที่จะจัดการเลือกตั้งประธานาธิบดีสหรัฐในปี 2020 เป็นต้น นอกจากนี้เรายังอาจพบเห็นภัยคุกคามทางไซเบอร์อื่น ๆ เช่น การใช้งานเพื่อการฉ้อโกงผ่านตัวตนที่สร้างขึ้นและการเกิดขึ้นขององค์กร deepfake-as-a-service ในปี 2020 อาจเป็นปีที่มีการหลอกลวงอย่างต่อเนื่องทำให้การหลอกลวงแบบฟิชชิงมีความน่าเชื่อถือมากขึ้นกว่าเดิม ซึ่งอาจทำให้ธุรกิจมีต้นทุนมากขึ้นหลายพันล้านดอลลาร์

7. มัลแวร์มือถือ (Mobile Malware)

ด้วยจำนวนผู้ใช้งานที่เพิ่มขึ้นเรื่อยๆ และค่อยๆ เคลื่อนย้ายจากระบบปฏิบัติการบนเดสก์ท็อปไปยังอุปกรณ์มือถือจำนวนข้อมูลทางธุรกิจที่จัดเก็บในช่วงหลังจะใหญ่ขึ้นเรื่อยๆ มัลแวร์มือถือเป็นซอฟต์แวร์ที่เป็นอันตรายที่ออกแบบมาเพื่อเป้าหมายระบบปฏิบัติการโทรศัพท์มือถือโดยเฉพาะ เนื่องจากมีการทำงานที่มีความสำคัญและละเอียดอ่อนมากขึ้นในสมาร์ทโฟนจึงเป็นเรื่องของเวลาก่อนที่มัลแวร์มือถือจะปรากฏเป็นหนึ่งในข้อกังวลด้านความปลอดภัยไซเบอร์ที่โดดเด่นที่สุด

8. ช่องโหว่ความปลอดภัย 5G-to-Wi-Fi

ความต้องการของบริษัทต่างๆ ในการหาวิธีใหม่ๆ ของการเพิ่มความปลอดภัยนั้นไม่เคยมีมากไปกว่านี้แล้ว เนื่องจากช่องว่างในเรื่องทักษะความปลอดภัยทางไซเบอร์และความซับซ้อนที่เพิ่มขึ้นของการโจมตีทางไซเบอร์ ไม่ต้องสงสัยเลยว่าผู้โจมตีจะพบช่องโหว่ใหม่ๆ ในการส่งข้อมูลผ่าน 5G-to-Wi-Fi ด้วยเครือข่าย 5G ที่เกิดขึ้นใหม่อย่างรวดเร็ว ทำผู้ให้บริการเครือข่ายไร้สายส่งข้อมูลหรือซอฟต์แวร์เพิ่มเติมไปยังเครือข่าย Wi-Fi ใช้ในการเสนอราคาเพื่อประหยัดแบนด์วิดท์ ช่องโหว่ของซอฟต์แวร์ในกระบวนการนี้เปิดโอกาสให้แฮกเกอร์เข้าโจมตีระบบรักษาความปลอดภัยต่างๆ

ด้วย 5G ที่เปิดตัวในพื้นที่สาธารณะที่กว้างขวาง เช่น สนามบิน ศูนย์การค้าและโรงแรม ข้อมูลเสียงและข้อมูลของผู้ใช้บนอุปกรณ์ ที่ใช้ระบบเซลลูลาร์จะได้รับการสื่อสารผ่านจุดเชื่อมต่อ Wi-Fi ในขณะที่อุปกรณ์มือถือมีความฉลาดในตัวเพื่อสลับระหว่างเครือข่ายเซลลูลาร์ และ Wi-Fi โดยอัตโนมัติ นักวิจัยด้านความปลอดภัยได้ระบุช่องโหว่จำนวนหนึ่งในกระบวนการนี้แล้ว มีความเป็นไปได้สูงว่าช่องโหว่ความปลอดภัย 5G-to-Wi-Fi ใหม่ที่สำคัญจะถูกเปิดเผยในปี 2020

9. ภัยคุกคามจากภายในองค์กร (Insider Threats)

รายงานการสอบสวนการละเมิดข้อมูลของ Verizon 2019 (DBIR) แสดงให้เห็นถึงการละเมิด ร้อยละ 34 เกี่ยวข้องกับคนภายในองค์กร การคุกคามจากภายในองค์กร ไม่เพียงแต่เกี่ยวข้องกับการโจมตีที่เป็นอันตรายเท่านั้นแต่ยังรวมถึงการใช้ระบบและข้อมูลโดยประมาท

/เพื่อป้องกัน...

เพื่อป้องกันภัยคุกคามเหล่านี้องค์กรจำเป็นต้องตรวจสอบ สอบสวนและตอบสนองต่อปัญหาที่อาจเป็นตัวบ่งชี้การโจมตีโดยใช้วงเครือข่ายภายในอย่างรวดเร็วและแม่นยำ เครื่องมือป้องกันไวรัสและมัลแวร์ทั่วไป (AV / AM) มักไม่มีประสิทธิภาพในการป้องกันภัยคุกคามเหล่านี้ ภัยคุกคามภายในต้องใช้เครื่องมือ (Tools) พิเศษเท่านั้น

เครื่องมือ (Tools) เหล่านี้ช่วยตรวจจับภัยคุกคามภายในได้โดยการตรวจสอบข้อมูล เช่น

- การเข้าสู่ระบบโดยไม่ได้รับอนุญาต
- แอปพลิเคชันต่างๆ ที่ติดตั้งบนคอมพิวเตอร์ที่ถูกล็อค
- ผู้ใช้ที่เพิ่งได้รับสิทธิ์ผู้ดูแลระบบไปยังอุปกรณ์
- อุปกรณ์บนเครือข่ายที่จำกัด และอื่นๆ

เครื่องมือต่างๆ เหล่านี้อาจจะรวมการเรียนรู้ของเครื่องและการติด Tag อัจฉริยะ (Agent) เพื่อระบุกิจกรรมที่ผิดปกติ การเปลี่ยนแปลงที่น่าสงสัยและการคุกคามที่เกิดจากการกำหนดค่าระบบผิดพลาด

10. ช่องโหว่และการละเมิดสิทธิ Application Programming Interface (API)

การศึกษาโดย Imperva บ่งชี้ว่าความพร้อมด้านความปลอดภัยของ application programming interface (API) มักจะช้ากว่าการรักษาความปลอดภัยเว็บแอปฯ ขององค์กรส่วนใหญ่ในปัจจุบัน นอกจากนี้มากกว่าสองในสามขององค์กรพร้อมให้บริการ API แก่สาธารณชนเพื่อให้นักพัฒนาและคู่ค้าภายนอกสามารถเข้าถึงระบบของแอพและแพลตฟอร์มซอฟต์แวร์ได้

เมื่อการพึ่งพา API เพิ่มขึ้นการละเมิด API จะกลายเป็นสิ่งที่โดดเด่นมากขึ้นในปี 2020 สิ่งนี้จะก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ต่อแอพพลิเคชั่นสูง ๆ ในกระบวนการทางการเงิน การส่งข้อความเพียร์ทูเพียร์ (P2P) ในขณะที่องค์กรจำนวนมากยังคงใช้ API สำหรับแอปพลิเคชันของตนต่อไปการรักษาความปลอดภัยบน API จะถูกเปิดเผย และเป็นจุดอ่อนซึ่งอาจนำไปสู่ภัยคุกคามบนคลาวด์ได้

วิธีการปฏิบัติเพื่อเพิ่มความปลอดภัยด้านไอทีเบื้องต้น

- ควรจัดการ อัปเดตแพทช์ (Patch) และช่องโหว่โดยอัตโนมัติ เพื่อให้ระบบไอทีขององค์กรมีความทันสมัยและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้เสมอ
- หมั่นสำรองข้อมูลระบบและข้อมูลแอป SaaS ขององค์กรเสมอ เพื่อให้แน่ใจว่าการกู้คืนมีประสิทธิภาพและรวดเร็วจากการโจมตี ransomware และการโจมตีอื่นๆ
- ปรับใช้โซลูชัน AV / AM ขั้นสูงเพื่อที่จะให้การตรวจจับปลายทางและการตอบสนอง (EDR) และทำให้ระบบของคุณปลอดภัย
- ตรวจสอบให้แน่ใจว่าแล็ปท็อปหรืออุปกรณ์ใดๆ ที่ออกจากสำนักงานมีการรักษาความปลอดภัยเต็มรูปแบบหรือไม่ เช่น ไฟร์วอลล์ การป้องกันมัลแวร์ขั้นสูงการกรอง DNS การเข้ารหัสดิสก์และการรับรองความถูกต้องแบบหลายปัจจัย เป็นต้น
- มีแผนรับมือเหตุการณ์ หากมีการละเมิดความปลอดภัยเกิดขึ้น องค์กรต้องมีแผนปฏิบัติการที่แข็งแกร่งเพื่อจัดการกับการละเมิดอย่างมีประสิทธิภาพ และนำองค์กรกลับคืนมาพร้อมกับความเสียหายขั้นต่ำและเร็วที่สุด แผนควรรวมถึงกลยุทธ์การสื่อสารสำหรับผู้มีส่วนได้เสียทั้งภายใน และภายนอกรวมถึงลูกค้านักลงทุนและอื่นๆ ยิ่งคุณเตรียมตัวล่วงหน้ามากเท่าไหร่คุณก็จะพร้อมรับมือกับวิกฤติได้ดีเท่านั้น

ข้อมูลจาก : https://www.kaseya.com/blog/2020/04/15/top-10-cybersecurity-threats-in-2020/

สรุปเรียบเรียงโดย : กลุ่มระบบคอมพิวเตอร์และความมั่นคงเครือข่าย กองสารสนเทศนิติวิทยาศาสตร์