INTERNALTIONAL ENGINEERING PROGRAMS

SRINAKHARINWIROT UNIVERSITY

http://inter.eng.swu.ac.th/

COMPUTER SECURITY & FORENSICS ENGINEERING INTRODUCTION

บทความนี้เรามาทำความรู้จักเบื้องต้นกับเรื่องราวของ Computer Security และ Digital Forensics สำหรับผู้ที่ไม่มีความรู้ด้านนี้มาก่อน

COMPUTER SECURITY & FORENSICS ENGINEERING คืออะไร

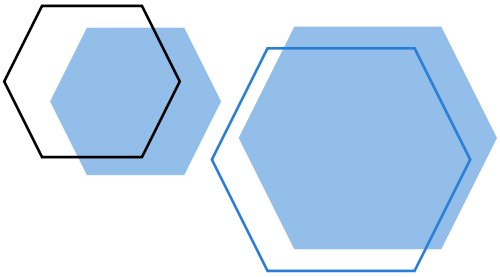
Computer Security (อาจเรียกว่า Cyber Security, Information System Security หรือ IT Security) คือศาสตร์ที่เกี่ยวข้องกับระบบรักษาความมั่นคงและปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ฮาร์ดแวร์และอุปกรณ์อิเล็คทรอนิคส์ต่างๆ ระบบให้บริการหรือแอปพลิเคชันต่างๆ รวมถึงข้อมูลสารสนเทศที่อยู่ในรูปดิจิ ทัล โดยเป้าหมายสำคัญ คือ เพื่อรักษาความลับ (Confidentiality) ความสมบูรณ์)Integrity) และความพร้อมใช้งาน)Availability (ของระบบหรือข้อมูลขององค์กร ซึ่งมีโอกาสที่จะถูกโจมตีทั้งโดยตั้งใจ และ ไม่ตั้งใจจากทั้งภายในและภายนอกองค์กร

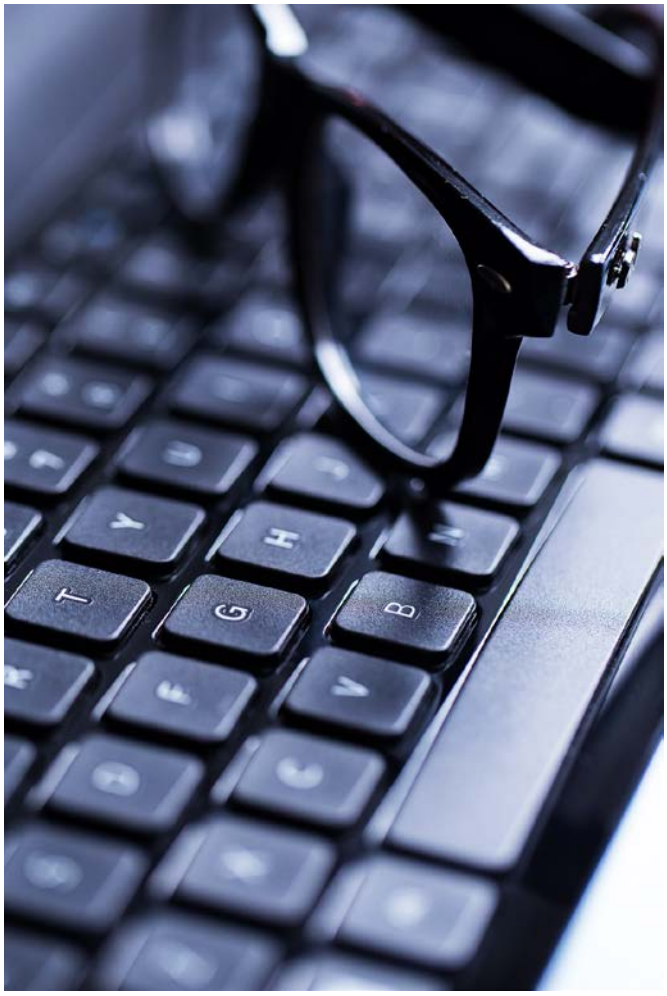
ส่วน Digital Forensics เป็นเรื่องที่เกี่ยวข้องกับระบบการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล เพื่อใช้ในการดำเนินคดีกับผู้กระทำผิด โดยการทำงานจะประกอบไปด้วย การรวมรวมพยานหลักฐาน การวิเคราะห์ และการรายงานผลการตรวจพิสูจน์ โดยจะต้องมีความถูกต้อง น่าเชื่อถือ และเป็นที่ยอมรับในชั้นศาล (Forensically Sound)

องค์ประกอบหลักที่เกี่ยวข้องได้แก่ เทคโนโลยี กระบวนการจัดการ และ บุคลากร โดยทั้งสามส่วนจะต้องทำงานประสานสอดคล้องกัน

1. เทคโนโลยี ได้แก่เครื่องมือต่างๆ ที่จะต้องมีความสามารถในการระงับ วิเคราะห์ ตรวจจับ แจ้งเหตุ ตามที่ได้รับการออกแบบและตั้งค่าไว้
2. กระบวนการจัดการ ได้แก่ นโยบายเกี่ยวกับความปลอดภัย มาตรฐาน แนวทางปฏิบัติ และขั้นตอนการปฏิบัติงาน ที่ถูกสร้างขึ้นและบังคับใช้ในองค์กร เพื่อให้สอดคล้องกับกลยุทธ์และความต้องการขององค์กร

บุคลากร จะต้องมีความรู้ความเข้าใจในหลักการที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์ กฎหมาย ระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง อีกทั้งยังต้องมีจิตสำนึกและจรรยาบรรณที่ถูกต้อง





ทำไม COMPUTER SECURITY & FORENSICS ถึงมีความสำคัญ

ในยุคดิจิทัลดิสรัปชัน (Digital Disruption) องค์กรต่าง ๆ พยายามที่จะ ปรับตัวเองให้ทันกับความเปลี่ยนแปลง และเพื่อให้สามารถแข่งขันได้ ไม่ถูก Disrupt โดยคู่แข่งที่อาจมีผลิตภัณฑ์คล้ายกัน หรือมาจากอุตสาหกรรมอื่นโดยบางบริษัทถึงกับต้องยอม Disrupt ตัวเอง เพื่อให้องค์กรยังเดินหน้าต่อไปได้ ตัวอย่างของการเปลี่ยนแปลงนี้ เช่น การเพิ่มช่องทางการเข้าถึงบริการผ่านทาง Internet เช่น ร้านค้าหรือผู้ผลิตสินค้าใช้บริการ E-commerce และ Logistics หรือธนาคารที่ให้บริการ Mobile Banking ให้ความสะดวกแก่ผู้ใช้ไม่ต้องไปใช้บริการที่สาขา รวมถึง บริการในรูปแบบใหม่ที่ไม่เคยมีมาก่อน เช่น Ride and accommodation share (Grab), E-Wallet/QR payment, Social trading, On-demand Music and VDO และอื่นๆ ทำให้องค์กรต้องพึ่งพาเทคโนโลยี และ ระบบทางดิจิทัลต่าง ๆ มากขึ้น ความมั่นคงปลอดภัยของระบบจึงเป็นสิ่งที่สำคัญอย่างยิ่งสำหรับทุกองค์กร

นอกเหนือจากนั้นการใช้บริการดิจิทัล ย่อมต้องมีการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้บริการและผู้ให้บริการ ทำให้มีข้อมูลเกิดขึ้นมากมาย ไม่ว่าจะเป็น ข้อมูลส่วนบุคคล ข้อมูลการใช้งาน ข้อมูลลิขสิทธิ์ และข้อมูลอื่นๆ ความก้าวหน้าทางเทคโนโลยีด้านข้อมูล (Data Science) ทำให้องค์กรต่าง ๆ สามารถใช้ประโยชน์จากข้อมูลเหล่านี้ในเชิงธุรกิจได้ องค์กรต่าง ๆ จึงมีความจำเป็นต้องมีการเก็บข้อมูลเหล่านี้ไว้ แต่ทว่า ข้อมูลเหล่านี้หากตกอยู่ในมืออาชญากรหรือถูกนำไปใช้ในทางที่ผิด อาจทำให้เกิดความเสียหายเกิดขึ้นแก่ทั้งผู้ใช้บริการ องค์กร หรือสังคมโดยรวม ทางภาครัฐในหลายๆประเทศจึงได้ออกกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลขึ้นมา เช่น General Data Protection Regulation (GDPR) โดยกลุ่มสหภาพยุโรป หรือ Personal Data Protection Act (PDPA) ของไทย องค์กรต่าง ๆ จึงมีหน้าที่ตามกฎหมายในการรักษาข้อมูลเหล่านี้ ให้ถูกใช้ตามวัตถุประสงค์ที่ได้ตกลงไว้กับผู้ใช้เท่านั้น และมีบทลงโทษที่ชัดเจนหากละเลย

ทำไม COMPUTER SECURITY & FORENSICS ถึงมีความสำคัญ (ต่อ)

จะเห็นได้ว่า Computer Security จึงกลายเป็นสิ่งสำคัญขององค์กรในยุคนี้ และเป็นสิ่งจำเป็นเพื่อปกป้ององค์กรจากเหตุการณ์การละเมิดความปลอดภัยทางไซเบอร์)Security breach) ที่มีโอกาสเกิดขึ้นตลอดเวลา โดยนักเจาะระบบ หรือ Hackers โดยอาศัยเทคนิคต่าง ๆ เช่น Spam URLs, Computer hacking, Malware, Anonymization service, Phishing, Botnet นอกเหนือจากความพยายามของ Hackers แล้ว การละเมิดยังสามารถเกิดขึ้นจากความไม่เป็นมืออาชีพของบุคลากรด้วย ในปี 2019 จำนวนการละเมิดทางข้อมูลหรือ Data Breach เพิ่มขึ้นถึง 33% หรือมีจำนวนข้อมูลที่ถูกเข้าถึงจากช่องโหว่)compromised(7.9 พันล้านครั้ง องค์กรต่าง ๆ เช่น Marriott, Facebook, Instagram, Armor, Games, American Medical Collection Association, Capital One, Adobe, etc. records

(ที่มา https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/)

ต่างได้รับผลกระทบจาก Data breach จากการประเมินโดย IBM การสูญเสียเฉลี่ยแต่ละครั้งของการละเมิดเป็นจำนวนเงินสูงถึง 3.92 ล้านเหรียญสหรัฐ

ความรู้และทักษะที่ COMPUTER SECURITY & FORENSICS ENGINEERS ต้องรู้มีอะไรบ้าง

เนื้อหาที่ต้องเรียนเพื่อให้มีความเชี่ยวชาญในการทำงานด้าน Computer security ประกอบด้วย ความเข้าใจพื้นฐานของระบบคอมพิวเตอร์ตั้งแต่ สถาปัตยกรรมระบบปฏิบัติการ ระบบเครือข่ายคอมพิวเตอร์ การเชื่อมต่อ Protocol ต่าง ๆ ,Programming หรือ Scripting language, Database, Web architecture, Web application โดยที่จะเน้นด้านความปลอดภัยทางคอมพิวเตอร์มากกว่าเนื้อหาของหลักสูตร Computer Engineering โดยทั่วไป

โดยในด้านความรู้เฉพาะทาง Computer Security & Forensics Engineers จะต้องมีความเข้าใจหลักการ ทฤษฎี เครื่องมือและเทคโนโลยี ที่เกี่ยวข้องกับ Computer security & forensics นอกเหนือจากนั้น ยังต้องมีความเข้าใจกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง มีทักษะในการประยุกต์ใช้ความรู้ ความสามารถให้เกิดประโยชน์สูงสุดต่อองค์กร

เนื่องจากComputer Security & Forensics Engineers เป็นผู้ที่มีความรอบรู้ทั้งการใช้ความรู้ในทางป้องกัน (Blue hat) การใช้ความรู้ในทางโจมตี (Red hat หรือ Ethical Hacking) สิ่งหนึ่งที่สำคัญที่สุดสำหรับ Computer Security & Forensics Engineers คือจะต้องมีจรรยาบรรณในวิชาชีพ ไม่ใช้ความรู้ความสามารถในทางที่ผิด เพราะความรู้ที่มีสามารถนำไปใช้เพื่อเกิดประโยชน์หรือนำไปใช้ให้เกิดความเสียหายได้อย่างมหาศาล เช่น ในกรณีที่ Hacker ขโมยข้อมูลบัตรเครดิต ทำให้เกิดความเสียหาย

จบแล้วสามารถทำงานอะไร และที่ไหนได้บ้าง

ตำแหน่งงานที่เกี่ยวข้องกับ Computer Security ในองค์กรส่วนใหญ่ได้แก่ Security Analyst, Security Consultant, Security Architect, Penetration Tester/Ethical Hacker, Chief Information Security Officer (CISO) จะเห็น Career path มีตั้งแต่ระดับแรกเข้า)Security analyst) ไปจนผู้บริหารระดับสูงขององค์กร (CISO) ซึ่งมีโอกาสที่จะก้าวขึ้นไปจนเป็น CIO (Chief Information Officer) ได้เช่นกัน

กลุ่มอุตสาหกรรมที่ต้องการบุคลากรด้าน IT Security อ้างอิงจากรายงานของ IBM เรื่อง 10 อุตสาหกรรมที่เป็นเป้าหมายในการโจมตีมากที่สุดในปี 2019 ได้แก่

1. Finance and Insurance

   ภาคการเงินและการประกันเป็นภาคอุตสาหกรรม ที่ตกเป็นเป้ามากที่สุด คิดเป็น 17% ของการโจมตีทั้งหมด โดยค่อนข้างจะชัดเจนสำหรับคนทั่วไปว่าทำไมผู้โจมตีถึงต้องการเจาะระบบ แต่ในขณะเดียวกันก็เป็นภาคอุตสาหกรรมที่มีความพร้อมในการป้องกันการโจมตีมากที่สุด เพราะฉะนั้นค่าเฉลี่ยการสูญเสียต่อเหตุการณ์อยู่ที่ $320,000 ซึ่งน้อยกว่าค่าเฉลี่ย $3.92 million รวมทุกกลุ่มอุตสาหกรรม

2. Retail

   เป็นภาคธุรกิจอันดับสอง สืบเนื่องจากการเติบโตของ e-Commerce โดยคิดเป็น 16% ของการโจมตีทั้งหมด การคุกคามส่วนใหญ่เกิดขึ้นเพื่อต้องการข้อมูลส่วนบุคคล ข้อมูลบัตรเครดิต ข้อมูลทางการเงิน ข้อมูลการจับจ่าย และ ข้อมูลแต้มสมาชิก โดยอาชญากรส่วนใหญ่ต้องการขโมยตัวตนลูกค้า (Identity theft) เทคนิคที่ใช้กันมากคือ Point-of-sale malware และ Card skimming และบาง ระบบอาจตกเป็นเป้าโจมตีโดยการฝัง Malicious Javascript ในหน้า website ที่มีการชำระเงิน ซึ่งสามารถส่งผลกระทบในวงกว้าง

จบแล้วสามารถทำงานอะไร และที่ไหนได้บ้าง (ต่อ)

3. Transportation

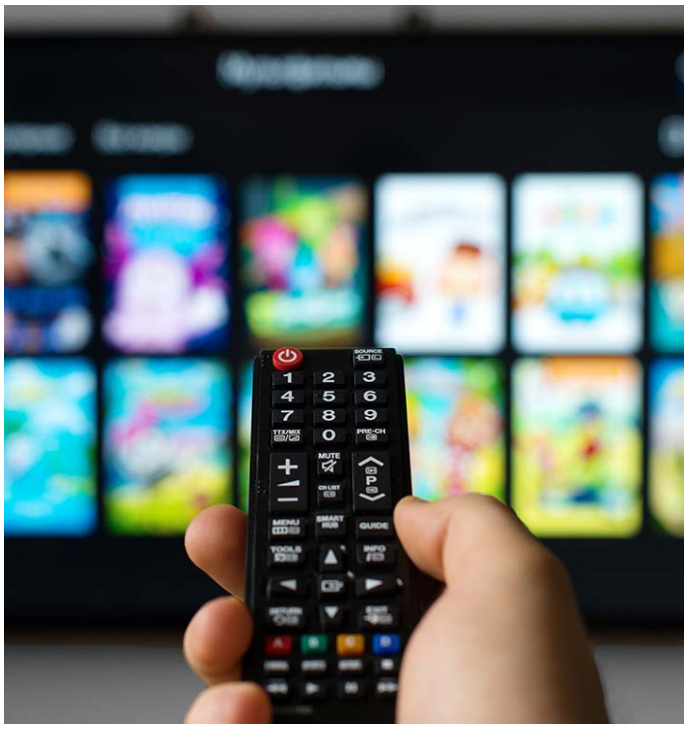
คิดเป็น1 0 %ของการโจมตีทั้งหมดได้แก่กลุ่มธุรกิจการขนส่ง ไม่ว่าจะเป็นทางบก ทางเรือ ทางอากาศ สำหรับผู้บริโภคและองค์กร ข้อมูลที่เป็นที่ต้องการสำหรับอาชญากรได้แก่ ข้อมูลระบุตัวตน)Personal Identifiable Information, PII) ข้อมูลชีวภาพ หมายเลข Passport ข้อมูล Loyalty program ข้อมูลบัตรชำระเงิน และ ข้อมูลแผนการเดินทาง ซึ่งสามารถถูกนำมาขายได้ใน Dark Web ข้อมูลพวกนี้มีความสำคัญเพราะสามารถทำให้เกิดความเสียหายต่อชีวิตของบุคคลสำคัญได้ กลุ่มที่โจมตีมีทั้งกลุ่มอาชญากรและจากหน่วยงานของรัฐที่เป็นปฏิปักษ์กัน

4. Media & Entertainment

อุตสาหกรรมนี้คือกลุ่มสื่อและการบันเทิง รวมถึงกลุ่มผู้ให้บริการการสื่อสาร ซึ่งเป็นเป้าหมายที่มีมูลค่าสูงสำหรับนักโจมตีระดับชาติที่ต้องการควบคุมการไหลของข่าวสาร การมีอิทธิพลต่อความคิดเห็นสาธารณะ หรือการปกป้องชื่อเสียงขององค์กรหรือของประเทศอื่น ๆ ส่วนอาชญากรรมก็คาดหวังจะได้รับผลตอบแทนจากการขโมย หรือ เรียกค่าไถ่ เนื้อหาลิขสิทธิ์

5. Professional services

กลุ่มนี้ประกอบด้วยธุรกิจที่ให้บริการในลักษณะให้คำปรึกษาเฉพาะด้าน ไม่ว่าจะเป็นกฎหมาย การบัญชี ภาษี ทรัพยากรบุคคล เป็นต้น คิดเป็น 10% ของการโจมตีทั้งหมด แต่จำนวนของข้อมูลที่ถูกละเมิดข้อมูลมีมากที่สุดในบรรดาทุกอุตสาหกรรม ซึ่งข้อมูลนั้นส่วนใหญ่คือข้อมูลของบริษัทคู่ค้า และเกิดขึ้นระหว่างการทำงานไม่ว่าจะเป็นเอกสารต่าง ๆ ซึ่งอาจถูกโจมตีโดยใช้ Macros หรือ Scripts ที่ฝังไว้ใน Files ต่าง ๆ

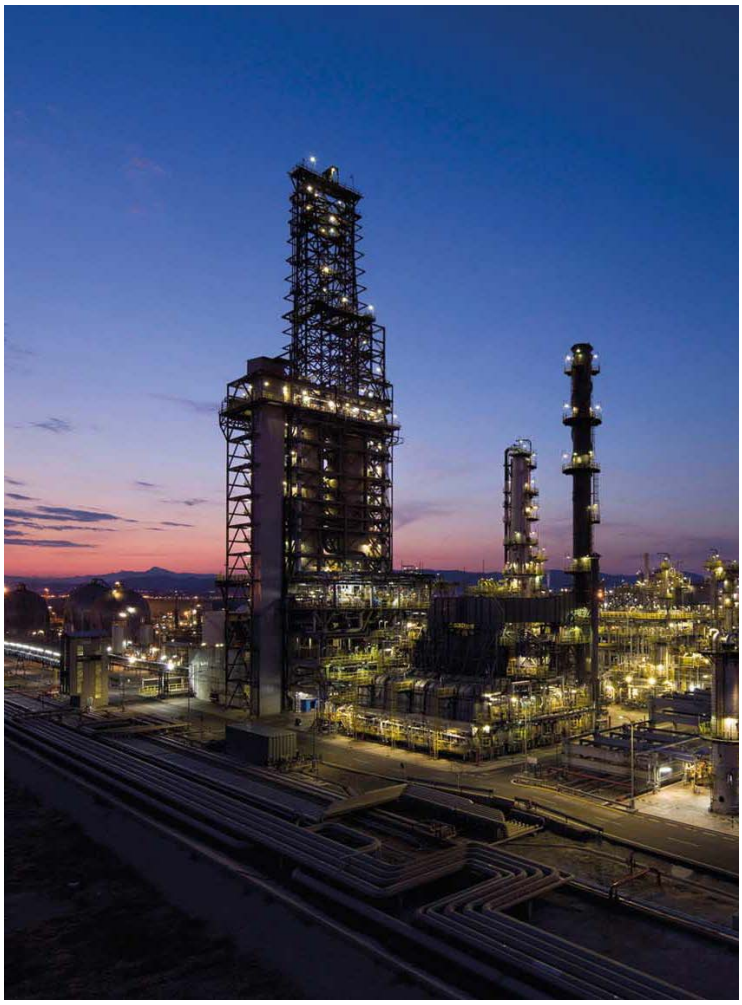


6. Government

หน่วยงานของรัฐ ตกเป็นเป้าหมายมากขึ้นโดยเลื่อนลำดับจากลำดับที่ 7 จากปี 2018 ภาคส่วนนี้เป็นเป้าหมายที่มีมูลค่าสูง โดยมีทั้งนักโจมตีระดับชาติที่มุ่งหวังเข้ามาทำลายหรือเจาะเอาข้อมูลที่ละเอียดอ่อนของชาติที่เป็นปฏิปักษ์ หรือจากนักโจมตีที่เป็นนักเคลื่อนไหวที่ต้องการแสดงความสามารถ และอาชญากรที่ต้องการเงินเรียกค่าไถ่เพื่อแลกกับข้อมูลที่ขโมยมา โดยหน่วยงานของรัฐในระดับท้องถิ่นตกเป็นเป้าหมายมากขึ้น เนื่องจากระบบรักษาความมั่นคงปลอดภัยที่ด้อยกว่าภาคเอกชน

7. Education

ภาคการศึกษาคิดเป็น 8% จากการโจมตีทั้งหมด เพิ่มขึ้นจาก 6% ในปี 2018 ข้อมูลที่เป็นที่ต้องการมีหลากหลาย ตั้งแต่ ทรัพย์สินทางปัญญา)IP) ไปจนข้อมูลระบุตัวตน)PII) ของนักศึกษาและบุคลากร วิธีการที่ใช้มากที่สุดยังได้แก่ Phishing e-mails เนื่องจากองค์กรการศึกษาส่วนใหญ่มี IT infrastructure และ Digital footprint ที่หลากหลาย จึงทำให้ช่องทางการโจมตีมีได้กว้าง ในประเทศสหรัฐอเมริกา ภายในเดือนตุลาคม 2019 เพียงเดือนเดียวมีโรงเรียนกว่า 500 แห่งที่ถูกเรียกค่าไถ่ข้อมูล นอกจากนี้ระบบเครือข่ายของมหาวิทยาลัยยังสามารถถูกใช้เป็นฐานในการเจาะเข้าระบบอื่น ๆ ที่เชื่อมโยง เช่น องค์กรการสื่อสาร โครงการกับภาครัฐ หรือ ทางด้านการทหาร



8. Manufacturing

ถึงแม้ว่าจะมีรายงานเกี่ยวกับการละเมิดข้อมูลที่เป็นข้อมูลสาธารณะจากภาคอุตสาหกรรมนี้น้อยกว่ากลุ่มอื่น แต่ไม่ได้แปลว่า การละเมิดข้อมูลอื่น ๆ จะไม่เกิดขึ้น)อาจไม่ได้ถูกเปิดเผย(การใช้ระบบ Operational Technology (OT) เช่น ICS หรือ SCADA ในการควบคุมระบบการผลิตทำให้อุตสาหกรรมนี้ตกเป็นเป้าการโจมตีเช่นกัน สิ่งที่ต้องการจากนักโจมตีได้แก่ เงิน หรือ ข้อมูลทรัพย์สินทางปัญญา โดยเทคนิคที่ถูกใช้มากที่สุดได้แก่ Business Email Compromise (BEC) fraud จากการแอบแฝงเป็นคู่ค้าข้ามชาติ เพื่อแอบยักยอกเงิน

9. Energy

บริษัทในกลุ่มพลังงานถือเป็นเป้าหมายที่ร่ำรวยสำหรับนักโจมตีทั้งจากอาชญากรและนักโจมตีของรัฐปฏิปักษ์ เนื่องจากความสำคัญของอุตสาหกรรมนี้ต่อความมั่นคงเชิงโครงสร้างของประเทศ เป็นอุตสาหกรรมที่มีผลกระทบต่อเศรษฐกิจ และการดำรงชีวิตของประชาชน เป้าหมายของการโจมตีของอุตสาหกรรมนี้ได้แก่ ข้อมูลลูกค้า ข้อมูลทางการเงิน ข้อมูลความลับองค์กร ข้อมูลเทคโนโลยีที่ไม่เปิดเผย ซึ่งคล้าย ๆกับของอุตสาหกรรมอื่น แต่ผลกระทบของการโจมตีนั้นมีโอกาสที่เกิดเป็นผลกระทบทางที่ร้ายแรง เช่น หากเกิดขึ้นกับโรงไฟฟ้าพลังงานปรมาณู หรือการที่การดำเนินงานขัดข้อง ทำให้เกิดผลกระทบในวงกว้างต่อธุรกิจอื่น ๆ ที่พึ่งพาพลังงาน ตัวอย่างในอดีตเช่น เหตุการณ์ที่เกิดขึ้นกับโรงไฟฟ้าในประเทศยูเครน โดยรัสเซียถูกกล่าวหาว่าเป็นผู้อยู่เบื้องหลัง

10. Healthcare

คิดเป็นสัดส่วนการโจมตี 3% ลดลงจาก 6% ในปี 2018 การโจมตีส่วนใหญ่ต้องการเงินจากการขายข้อมูล Medical records ใน Dark Web หรือการเรียกค่าไถ่จากการปั่นป่วนอุปกรณ์ให้ทำงานผิดปกติ โดยมีกรณีของ 2019 Ryuk attack ที่มีการจ่ายค่าไถ่เป็นจำนวนถึง $14 ล้านเหรียญเพื่อให้ระบบกลับมาใช้งานได้และปกป้องชีวิตของผู้ป่วย ในปี 2020 กลุ่มอุตสาหกรรมการดูแลสุขภาพยังคงต้องพัฒนาด้านการปกป้องข้อมูลให้ดีขึ้นเรื่อย ๆ ยังดีที่ไม่พบการเคลื่อนไหวของนักโจมตีของรัฐปฏิปักษ์ในกลุ่มอุตสาหกรรมนี้

สรุป

บุคลากรด้าน Computer Security เป็นที่ต้องการเป็นอย่างมากในโลกยุคดิจิทัล จากทั้งภาครัฐและเอกชนในอุตสาหกรรมด้านต่าง ๆ ไม่ใช่เฉพาะด้านการเงินการธนาคารเท่านั้น แต่รวมถึง การค้าปลีก การขนส่ง การผลิตสื่อและความบันเทิง การบริการทางวิชาชีพ การศึกษา การผลิต การพลังงาน และการดูแลสุขภาพ

ถึงแม้ว่าทักษะพื้นฐานอาจจะคล้ายกับบัณฑิตที่จบด้าน Computer Engineering หรือ Computer Science แต่คนที่จะทำด้าน Security ได้จะต้องได้รับการศึกษาเฉพาะทาง เพื่อให้มีความเข้าใจอย่างลึกซึ้งและมีทักษะที่สามารถนำไปปฏิบัติงานได้ โดยส่วนใหญ่แล้วหลักสูตร Computer Security จะเป็นในระดับปริญญาโท สำหรับผู้ที่มีพื้นฐานด้านคอมพิวเตอร์มาก่อน

แต่สำหรับน้อง ๆ ที่กำลังจะจบชั้นมัธยมที่สนใจต้องการเรียนรู้ด้านนี้ ทางมหาวิทยาลัยศรีนครินทร์วิโรฒ โดยกลุ่มหลักสูตรวิศวกรรมนานาชาติ ได้เปิดหลักสูตร Computer Security and Forensics Engineering ในระดับปริญญาตรี หลักสูตรนานาชาติ สำหรับนักเรียน นักศึกษา ที่ไม่จำเป็นต้องมีพื้นฐานด้านคอมพิวเตอร์มาก ไม่จำเป็นต้องเขียน program มาก่อน แต่มีความสนใจ ต้องการความท้าทายและยึดถือในสิ่งที่ถูกต้อง โดยเป็นหลักสูตรนานาชาติและได้รับสองปริญญาจากทั้ง มศว และ De Monfort University ภายในเวลา 4 ปีก็สามารถจบออกมาทำงานได้เลย ถือเป็นอีกทางเลือกหนึ่งที่น่าสนใจ

REFERENCE

https://en.wikipedia.org/wiki/Computer_security

https://www.thaicert.or.th/papers/general/2013/pa2013ge012.html#3

https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

https://www.helpnetsecurity.com/2019/11/14/breaches-2019/

https://en.wikipedia.org/wiki/(ISC)²

https://www.ibm.com/security/services/ibm-x-force-incident-response-and-intelligence