

# ทีมวิศวลาดกระบัง คว่ำรางวัลความปลอดภัยไซเบอร์ จากเวที KPMG Cyber Security Challenge มาเลเซีย



ในยุคดิจิทัล ทรานส์ฟอร์มเมชัน เราได้ยินข่าวบ่อยครั้งว่ามีโจรไซเบอร์แฮ็คเจาะข้อมูลสร้างความเสียหายมหาศาลให้กับองค์กรและธุรกิจการดำเนินงานมากมาย ดังนั้นแม้ดิจิทัลเทคโนโลยีนำมาซึ่งความเปลี่ยนแปลงในวิถีชีวิต การทำงาน การศึกษาและแพลตฟอร์มการทำธุรกิจใหม่ๆเกิดขึ้นมากมายได้นำมาซึ่งความสะดวกสบาย ชีวิตที่ทันสมัยและประสิทธิภาพ แต่ก็ยังมีภัยทางไซเบอร์ตามมาด้วย ล่าสุด ในการจัดแข่งขัน KPMG Cyber Security Challenge 2017 ณ ศูนย์ CCEC (Connexion Conference & Event Centre ) เมืองกัวลาลัมเปอร์ ประเทศมาเลเซีย ผลปรากฏว่า ทีม 555 พลัส จากคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) ได้รับรางวัลรองชนะเลิศอันดับที่ 1

รศ.ดร.คมสัน มาลีสี คณบดี คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) กล่าวว่า การแข่งขัน KPMG Cyber Security Challenge เป็นเวทีประลองทักษะและความสามารถในการปลอดภัยไซเบอร์ในด้านการตรวจสอบพิสูจน์หลักฐานทางคอมพิวเตอร์ (Digital Forensics) การตรวจสอบช่องโหว่ของเว็บและโมบายแอปพลิเคชัน (Mobile and Web Application Exploitation) ช่องโหว่ของระบบเครือข่ายและระบบปฏิบัติการ (Network and System Exploitation) การวิเคราะห์การทำงานของมัลแวร์ (Malware Analysis) การทำวิศวกรรมย้อนกลับ (Reverse Engineering) การเข้ารหัส (Cryptography) และการรักษาความปลอดภัยทางกายภาพ (Physical Security) เพื่อวิเคราะห์และแก้ปัญหาโจทย์ต่างๆ จัดโดย เคพีเอ็มจี โดยมีวัตถุประสงค์เพื่อส่งเสริมศักยภาพความสามารถของเยาวชน พัฒนาการป้องกันการแฮคข้อมูลและยกระดับความปลอดภัยทางดิจิทัล เนื่องจากปัจจุบันมีเทคโนโลยีเกิดขึ้นใหม่มากมาย ซึ่งไม่ได้จำกัดเพียงคอมพิวเตอร์อีกต่อไปแล้ว บรรดาของใช้ภายในบ้านได้กลายเป็นอุปกรณ์เครื่องใช้อัจฉริยะด้วยนวัตกรรมไอโอที เทคโนโลยีซึ่งช่วยให้ชีวิตของเราสามารถเชื่อมและติดต่อสื่อสารกันได้ง่ายอย่างที่ไม่เคยเกิดขึ้นมาก่อน ขณะเดียวกัน เทคโนโลยียังเพิ่มอัตราความเสี่ยงในการถูกโจมตีทางไซเบอร์ในชีวิตประจำวันมากขึ้น ทั้งยังช่วยเผยแพร่ความรู้ให้เยาวชนได้ตระหนักถึงความสำคัญของความปลอดภัยในโลกไซเบอร์อีกด้วย

อิสรา นรานิรัตติย์ หรือ ดริ่ม หนุ่ม นักศึกษาหัวหน้าทีมไทย ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สจล. กล่าวว่า ทีมของเราได้เข้าแข่งขันรายการ KPMG Cyber Security Challenge ที่ประเทศมาเลเซีย มีสมาชิก

ในทีมมี 4 คนคือ ตัวผมเอง ,นายเมธาสิทธิ์ รินทร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ , นายชรรต แสงสมเรือง ภาควิชาเทคโนโลยีสารสนเทศ, นายกมนนพ อรุณรัตน์ ภาควิชาวิศวกรรมคอมพิวเตอร์ และมีผศ. อัครเดช วัชรระภูพงษ์ เป็นอาจารย์ผู้ควบคุมทีม ในการแข่งขันจะมีโจทย์ต่างๆ เพื่อทดสอบทักษะด้านความปลอดภัยทางไซเบอร์ โดยจะเป็นโจทย์ให้ทำเรียงลำดับเป็นข้อๆ ความท้าทายอยู่ที่เมื่อได้คำตอบในข้อปัจจุบันจะเป็นเบาะแสเพื่อหาคำตอบในข้อถัดไป สำหรับเกณฑ์การตัดสินดูจากคะแนนที่ได้จากการหาคำตอบและเวลาที่ส่งคำตอบที่เร็วที่สุดในกรณีที่ได้คะแนนเท่ากัน ทีมวิศวลาดกระบัง สจล.ได้เตรียมตัวมาอย่างหนักโดยการหาโจทย์เก่าๆและโจทย์จากการแข่งขันในรายการอื่นๆมาฝึกซ้อม

ประสบการณ์ที่เราได้รับจากการไปแข่งขันครั้งนี้จะนำมาพัฒนาใช้ประโยชน์สำหรับบ้านเรา มีโอกาสได้รู้จักมืออาชีพในวงการความปลอดภัยทางไซเบอร์ (Cyber Security) ทั้งชาวไทยและต่างชาติ ได้ฝึกประสบการณ์จากการแข่งขัน และได้เพิ่มพูนความรู้ทางด้าน Cyber มากขึ้น และการทำงานเป็นทีมกับเพื่อนๆ ทำให้เกิดความสามัคคีในทีมเป็นอย่างมาก เพราะขั้นตอนการแข่งขันต้องช่วยกันระดมความคิด เพื่อวิเคราะห์และแก้ปัญหาโจทย์ต่างๆ ในเวลาเดียวกันยังช่วยแก้การเข้ารหัสแฉกข้อมูล นำมาประยุกต์ใช้ซึ่งทำให้ทราบถึงกลวิธีและจุดอ่อนของตนล่วงหน้าเพื่อหาทางป้องกันก่อนที่ผู้ประสงค์ร้ายจะกระทำการไม่ดีต่อระบบ อาชญากรรมทางไซเบอร์มีจำนวนเพิ่มขึ้นทั่วโลกอย่างต่อเนื่อง ในเวลาเพียงไม่กี่เดือนที่ผ่านมา การโจมตีทางระบบความปลอดภัยไซเบอร์ เกิดเป็นช่องโหว่จากความมั่นคงปลอดภัยด้านไซเบอร์อยู่ในระดับสูงสุดอย่างเป็นประวัตินการณ์ และเป็นปัญหาที่เกิดขึ้นมายาวนาน

ดริม ให้มุมมองว่า เทคโนโลยีนั้นมี 2 ด้าน ประโยชน์มากล้น แต่ก็มีความเสี่ยงในการใช้คอมพิวเตอร์อย่างปลอดภัย เช่น ควรตรวจสอบความปลอดภัยอยู่อย่างสม่ำเสมอ ไม่ติดตั้งหรือดาวน์โหลดซอฟต์แวร์ต่างๆที่มีความเสี่ยง และรักษาความเป็นส่วนตัว ไม่ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ การตั้งรหัสผ่านต่างๆให้มีความยากต่อการเดา เพราะวิธีการของแฮกเกอร์จะหาจุดอ่อนหรือช่องโหว่ของระบบ จากนั้นก็จะเจาะเข้ามาในเซิร์ฟเวอร์และเข้ามาทำความเสียหายให้กับข้อมูล

นอกจากนี้ควรมีข้อปฏิบัติที่ดี 1.ติดตั้งซอฟต์แวร์รักษาความปลอดภัย 2. ตั้งค่าระบบ IT ให้มีความรัดกุม 3. สำรองข้อมูลอย่างสม่ำเสมอ 4. กำหนดสิทธิของผู้ใช้ และ 5. จัดการสภาพแวดล้อมทาง IT ให้เป็นระบบปิดมากที่สุด