ความมั่นคงปลอดภัยทางไซเบอร์

(Cyber Security)

หลักการและเหตุผล

ความก้าวหน้าด้านเทคโนโลยีสารสนเทศ และการสื่อสาร รวมไปถึงเครือข่ายโซเชียลต่าง ๆ มีบทบาทอย่างมากในชีวิตประจำวันของคนยุคปัจจุบัน ขณะเดียวกันพบว่าปัญหาความปลอดภัยทางไซเบอร์ก็ได้ทวีความเข้มข้น และมีความรุนแรงมากขึ้นตามลำดับ ซึ่งภัยคุกคามไซเบอร์มีผลกระทบทั้งระดับชาติ ระดับองค์กร องค์กรจึงต้องพัฒนากำลังคนเพื่อให้มีความรู้ความสามารถในการปกป้ององค์กรให้ปลอดภัยจากภัยไซเบอร์ในรูปแบบต่าง ๆ หลักสูตรความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) มีเนื้อหาเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ การออกแบบระบบเทคโนโลยีสารสนเทศขององค์กรให้ปลอดภัย การรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling) และเป็นจุดเริ่มต้นของทักษะทางด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศในระดับมืออาชีพ

วัตถุประสงค์การอบรม

1. เพื่อให้ผู้อบรมมีความรู้ในเรื่องหลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์
2. เพื่อให้ผู้อบรมมีความรู้ในเรื่องการรักษาความปลอดภัยให้กับระบบเครือข่าย
3. เพื่อให้ผู้อบรมมีความรู้ในเรื่องเทคโนโลยี Endpoint Security
4. เพื่อให้ผู้อบรมมีความรู้ในเรื่องการประเมินช่องโหว่ของระบบและการบริหารจัดการความเสี่ยง
5. เพื่อให้ผู้อบรมมีความรู้ในเรื่องการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

คุณสมบัติผู้เข้ารับการอบรม

1. สามารถใช้งานคอมพิวเตอร์และอินเทอร์เน็ตได้เป็นอย่างดี
2. มีความรู้พื้นฐานในเรื่องอุปกรณ์คอมพิวเตอร์และอุปกรณ์ภายในระบบเครือข่าย (Network)

ระยะเวลาการอบรม

3 วัน (18 ชั่วโมง)

ลักษณะและวิธีการฝึกอบรม

เป็นการบรรยาย และสาธิตแต่ละเนื้อหาผ่านแบบฝึกปฏิบัติ กับเครื่องคอมพิวเตอร์ 1 คน ต่อ 1 เครื่อง

เนื้อหาการอบรม วันที่ 1

09:00 – 10:30 น. **หลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์**

- ความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน (Cyber Security Principles)

10:30 – 10:45 น. พักรับประทานอาหารว่าง (เช้า)

10:45 – 12:00 น. **หลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์**

- ภัยคุกคามและช่องโหว่ (Threats and Vulnerabilities)

12:00 – 13:00 น. พักรับประทานอาหารกลางวัน

13:00 – 14:30 น. **หลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์**

- การบริหารจัดการการเข้าถึงระบบ (Access Control)
- เทคโนโลยีการเข้ารหัส (Encryption)

14:30 – 14:45 น. พักรับประทานอาหารว่าง (บ่าย)

14:45 – 16:00 น. **หลักการพื้นฐานการรักษาความปลอดภัยให้กับระบบเครือข่าย**

- ช่องโหว่ของโพรโทคอล TCP/IP
- การวางแผนผังระบบเครือข่ายให้มีความมั่นคงปลอดภัย

เนื้อหาการอบรม วันที่ 2

09:00 – 10:30 น. **หลักการพื้นฐานการรักษาความปลอดภัยให้กับระบบเครือข่าย**

- โครงสร้างพื้นฐานและเทคโนโลยีของระบบเครือข่าย
- การติดตั้งระบบเครือข่ายไร้สายที่มีความมั่นคงปลอดภัยให้กับสำนักงานขนาดเล็ก
- การติดตั้งและการควบคุมการเข้าถึง (Access Control) ระบบเครือข่ายให้มีความมั่นคงปลอดภัย

10:30 – 10:45 น. พักรับประทานอาหารว่าง (เช้า)

10:45 – 12:00 น. **หลักการเทคโนโลยี Endpoint Security**

- การรักษาความมั่นคงปลอดภัยให้กับระบบปฏิบัติการ
- การใช้เครื่องมือ Security Endpoint เพื่อเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- คุณสมบัติของเครื่องมือ Security Endpoint ตามมาตรฐานและนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์

12:00 – 13:00 น. พักรับประทานอาหารกลางวัน

13:00 – 14:30 น. **หลักการเทคโนโลยี Endpoint Security**

- การอัปเดตซอฟต์แวร์และฮาร์ดแวร์ (Implement software and hardware updates)
- การวิเคราะห์และแปลผล Logs
- การกำจัดมัลแวร์

14:30 – 14:45 น. พักรับประทานอาหารว่าง (บ่าย)

14:45 – 16:00 น. **การประเมินช่องโหว่ของระบบและการบริหารจัดการความเสี่ยง**

- การบริหารจัดการช่องโหว่ของระบบ
- การใช้ข่าวกรองด้านภัยคุกคามไซเบอร์ (Threat Intelligence) เพื่อหาช่องโหว่ของระบบที่มีความเป็นไปได้

เนื้อหาการอบรม วันที่ 3

09:00 – 10:30 น. **การประเมินช่องโหว่ของระบบและการบริหารจัดการความเสี่ยง**

- การบริหารจัดการความเสี่ยง (Risk Management)
- แผนกู้คืนภัยพิบัติ (DR Plan) และแผนบริหารความต่อเนื่อง (BCP Plan)

10:30 – 10:45 น. พักรับประทานอาหารว่าง (เช้า)

10:45 – 12:00 น. **การรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling)**

- การรับมือกรณีเมื่อเกิดเหตุการยกระดับสิทธิ (Privilege Escalation)
- การพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensic) และกระบวนการพิสูจน์พยานหลักฐานทางดิจิทัล

12:00 – 13:00 น. พักรับประทานอาหารกลางวัน

13:00 – 14:30 น. **การรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling)**

- กรอบการปฏิบัติตามกฎหมายและระเบียบ (Compliance Frameworks) ที่เกี่ยวข้องกับการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- องค์ประกอบของการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

14:30 – 14:45 น. พักรับประทานอาหารว่าง (บ่าย)

14:45 – 16:00 น. LAB: การประเมินช่องโหว่ (Vulnerability Assessment) ระบบปฏิบัติการ