เฝ้าระวังภัยคุกคามทางไซเบอร์ตลอดเวลาด้วยศูนย์รักษาความปลอดภัย SOC

ปัจจุบันการทำธุรกรรมต่าง ๆ บนอินเทอร์เน็ตมีการใช้งานอย่างแพร่หลาย และขยายตัวอย่างต่อเนื่อง ไม่ว่าจะเป็นการใช้งานทั่วไป เช่น โซเชียลมีเดีย การสืบค้น และรับส่งข้อมูล รวมถึงการทำธุรกรรมทางการเงินที่ต้องการความถูกต้องของข้อมูล และความปลอดภัยสูง เช่น การโอนเงิน และชำระค่าสินค้าหรือบริการ อ้างอิงจากผลสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ต ปี 2561 ของ ETDA พบว่าคนไทยส่วนใหญ่ใช้อินเทอร์เน็ตเฉลี่ยนานขึ้นถึง 10 ชั่วโมง 5 นาทีต่อวัน ซึ่งเพิ่มขึ้นจากปีก่อนถึง 3 ชั่วโมง 41 นาทีต่อวัน ส่งผลให้ภัยคุกคามทางไซเบอร์เติบโต และพัฒนาขึ้นด้วยเช่นกัน ซึ่งจากสถิติของ ThaiCERT ปี 2562 พบว่าประเทศไทยครองอันดับ 3 ของโลกที่แจ้งเหตุภัยคุกคามมากที่สุด ทำให้องค์กร และหน่วยงานต่าง ๆ ตกอยู่ในความเสี่ยงที่เพิ่มสูงขึ้น จึงจำเป็นที่จะต้องมีความตื่นตัวมากขึ้น เพราะภัยคุกคามทางไซเบอร์ สามารถสร้างความเสียหายอย่างมหาศาลต่อธุรกิจ ไม่ว่าจะเป็นการโจมตีระบบหรือการบุกรุกทำลายข้อมูลสำคัญขององค์กร ดังนั้น การมองหาโซลูชันในการรักษาความปลอดภัยด้านไอทีแบบครบวงจรจึงเป็นเรื่องสำคัญ โดยหนึ่งในการดำเนินการที่องค์กรควรพิจารณา คือ Security Operation Center หรือ SOC ซึ่งเป็นศูนย์รักษาความปลอดภัยระบบ IT ซึ่งจะช่วยรักษาความปลอดภัย และป้องกันภัยคุกคามทางไซเบอร์ได้อย่างไรนั้น เราไปดูพร้อมกัน!

Security Operation Center หรือ SOC คือ ศูนย์รักษาความปลอดภัยระบบเครือข่าย และเทคโนโลยีสารสนเทศ ถ้าจะให้อธิบายง่าย ๆ ศูนย์รักษาความปลอดภัย SOC เปรียบเสมือนยามที่คอยเฝ้าระวัง และป้องกันระบบของคุณจากการถูกบุกรุกตลอด 24 ชั่วโมง หากเกิดเหตุการณ์ที่ผิดปกติ หรือเหตุการณ์ที่สนใจตามเงื่อนไขจะทำการแจ้งเตือน เพื่อให้คุณสามารถรับมือกับเหตุการณ์นั้นได้ทันท่วงที โดยทางบริษัท ไอเน็ต แมเนจด์ เซอร์วิสเซส จำกัด

บริษัทในเครือ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) หรือ INET ได้ให้บริการ INETMS SOC ซึ่งเป็นบริการตรวจสอบ เฝ้าระวัง และแจ้งเตือน เมื่อพบพฤติกรรมที่เป็นภัยคุกคาม หรือเหตุการณ์ที่ผิดปกติ พร้อมให้คำแนะนำในการรับมือ แก้ไขปัญหา รวมถึงแนวทางการป้องกัน ผ่านศูนย์รักษาความปลอดภัย SOC โดยมีทีมงานผู้เชี่ยวชาญที่มีความรู้ และประสบการณ์คอยดูแลตลอดเวลา (24×7) โดยการทำงานของศูนย์รักษาความปลอดภัย SOC คือ ทำการวิเคราะห์ log ที่ผ่านเข้ามา หากพบว่ามีแนวโน้มที่จะเป็นเป็นภัยคุกคามต่อระบบก็จะทำการแจ้งเตือนก่อนที่จะถูกโจมตี ซึ่ง INETMS SOC ได้นำเทคโนโลยีที่ทันสมัยเข้ามาเพื่อความปลอดภัยขั้นสุดไม่ว่าจะเป็น

- การนำระบบ AI มาช่วยวิเคราะห์พฤติกรรมเพื่อสู้กับ Hacker ในยุคดิจิตอล เพราะกลุ่มอาชญากรในโลกไซเบอร์นั้นจะมีความฉลาดล้ำขึ้นเรื่อย ๆ มีการหลบหลีก และใช้วิธีการรูปแบบใหม่ ๆ อยู่เสมอ การนำ AI เข้ามาจะช่วยให้การวิเคราะห์ log แม่นยำยิ่งขึ้น
- การอัพเดทช่องโหว่ใหม่ ๆ จากทั่วโลกอยู่เสมอด้วย Thread intelligent เพื่อให้ทราบว่าเรากำลังเผชิญกับภัยคุกคามทางไซเบอร์อะไรบ้าง ทำให้ระบบคอมพิวเตอร์ของคุณปลอดภัยทั้งจากภัยคุกคามที่รู้จักกันดีอยู่แล้ว และภัยคุกคามรูปแบบใหม่ๆที่เพิ่งถูกค้นพบอีกด้วย
- การนำส่งรายงานประจำเดือน เพื่อรายงานว่ามีเหตุการณ์อะไรเกิดขึ้นบ้าง พร้อมให้คำแนะนำในการป้องกันภัยคุกคามนั้น ๆ นอกจากนี้ยังมีการอัพเดท และแจ้งเตือนถึงข่าวการโจมตี และช่องโหว่ใหม่ ๆ อีกด้วย
- บริการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๐ (Add-on)

ภัยคุกคามทางไซเบอร์ สามารถสร้างความเสียหายทางธุรกิจได้อย่างน่าตกใจ การเฝ้าระวังแบบเชิงรุก จึงเป็นเรื่องจำเป็น มาเฝ้าระวังระบบของคุณให้มีความมั่นคงปลอดภัยอยู่ตลอดเวลาด้วย INETMS SOC ประหยัดทั้งค่าใช้จ่ายไม่ต้องลงทุน Software Hardware และบุคลากร สามารถเพิ่ม-ลดได้ตามปริมาณการใช้งานจริงในราคาที่เอื้อมถึง ด้วยการให้บริการแบบมืออาชีพด้วยทีมงานที่มีประสบการณ์ และความเชี่ยวชาญสูง ได้รับมาตรฐานระดับสากล หากสนใจสามารถติดต่อเพิ่มเติมได้ที่ marketing@inet.co.th