แคสเปอร์สกี้ให้โรงพยาบาลใช้ฟรี 6 เดือน ลุยฝ่าวิกฤตโควิด-19

แคสเปอร์สกี้ประกาศให้หน่วยงานด้านสาธารณสุขสามารถใช้โปรดักส์เพื่อความปลอดภัยองค์กรของแคสเปอร์สกี้ได้โดยไม่มีค่าใช้จ่ายนานหกเดือน เพื่อช่วยให้หน่วยงานสามารถป้องกันภัยไซเบอร์ได้ในสถานการณ์โรคระบาดในปัจจุบัน โปรดักส์ที่ร่วมได้แก่ Kaspersky Endpoint Security Cloud Plus, Kaspersky Security for Microsoft Office 365, Kaspersky Endpoint Security for Business Advanced และ Kaspersky Hybrid Cloud Security

ความต่อเนื่องของการดำเนินงานและความปลอดภัยของข้อมูลเป็นเรื่องจำเป็นอย่างยิ่งสำหรับหน่วยงานด้านสาธารณสุข โดยเฉพาะในสถานการณ์ปัจจุบัน เมื่อหน่วยงานสาธารณสุขต่างต้องทำงานท่ามกลางความกดดันและใช้พละกำลังเพื่อช่วยเหลือประชาชน เครื่องมือทางการแพทย์ในโรงพยาบาลจำเป็นต้องทำงานอย่างต่อเนื่อง และข้อมูลส่วนตัวของผู้ป่วยก็เป็นอีกสิ่งที่โรงพยาบาลต้องปกป้องเช่นกัน

“ในช่วงวิกฤตนี้ หน่วยงานการแพทย์ทำงานท่ามกลางความกดดันหลายด้าน อีกทั้งยังแบกความรับผิดชอบเพื่อรักษาชีวิตของผู้ป่วยและต่อสู้กับการแพร่ระบาดนี้ หมอ พยาบาล และเจ้าหน้าที่การแพทย์ต่างมีงานล้นมือและต้องการการสนับสนุนมากที่สุดเท่าที่จะเป็นไปได้ นี่เป็นหนึ่งในหน้าที่ของแคสเปอร์สกี้เพื่อสนับสนุนวงการแพทย์” เอฟจีนิย่า นอโมวา รองประธานฝ่ายเครือข่ายการขายระดับโลก บริษัทแคสเปอร์สกี้ กล่าว “เพื่อให้หน่วยงานการแพทย์ได้พุ่งความสนใจไปที่สิ่งสำคัญที่สุด แคสเปอร์สกี้จึงขอเสนอให้หน่วยงานได้ใช้โปรดักส์องค์กรของเราได้โดยไม่มีค่าใช้จ่าย

ใดๆ นานหกเดือน”

หน่วยงานที่สนใจสามารถดูข้อมูลเพิ่มเติมได้ที่

https://www.kaspersky.com/blog/protecting-healthcare-organizations/ และ
https://www.kaspersky.co.th/

นอกจากนี้ แคสเปอร์สกี้ยังได้แนะนำมาตรการเพื่อความปลอดภัยทางไซเบอร์สำหรับหน่วยงานการแพทย์ดังนี้

1. ให้ความรู้ความเข้าใจพื้นฐานด้านความปลอดภัยไซเบอร์แก่บุคลากรการแพทย์ รวมถึงพนักงานธุรการของโรงพยาบาล ซึ่งรวมถึงการอบรมที่จำเป็นอย่างพาสเวิร์ด แอคเค้าท์ ความปลอดภัยของอีเมล การใช้ USB ดีไวซ์ ความปลอดภัยของคอมพิวเตอร์ และการใช้เว็บให้ปลอดภัย และควรอธิบายให้พนักงานเข้าใจถึงความเสี่ยงของภัยคุกคามไซเบอร์ต่อระบบไอทีของหน่วยงานสาธารณสุข
2. ตรวจสอบโซลูชั่นความปลอดภัยของโรงพยาบาล โดยโซลูชั่นที่ใช้งานอยู่จะต้องเป็นเวอร์ชั่นล่าสุดอยู่เสมอ มีการตั้งค่าที่เหมาะสมครอบคลุมดีไวซ์ต่างๆ ของพนักงาน เปิดใช้งานไฟร์วอลล์เพื่อป้องกันภัยจากอินเทอร์เน็ต และควรมีฟีเจอร์ป้องกันแรนซัมแวร์ซึ่งเป็นภัยคุกคามที่มักจ้องเล่นงานหน่วยงานการแพทย์ตลอดเวลา
3. ตรวจสอบอุปกรณ์ทางการแพทย์ เช่น เครื่องช่วยหายใจ ซึ่งควรอัพเดทอย่างสม่ำเสมอ หากจำเป็นต้องเพิ่มจำนวนอุปกรณ์ต่างๆ อย่างรวดเร็ว จะต้องมีขั้นตอนการติดตั้งอุปกรณ์ใหม่ที่รวดเร็วเช่นกัน
4. โรงพยาบาลหลายแห่งจำเป็นต้องจ้างพนักงานใหม่เพิ่ม ซึ่งหมายถึงการเพิ่มจำนวนเครื่องคอมพิวเตอร์และดีไวซ์ส่วนตัวของพนักงาน ที่อาจกระทบต่อการควบคุมด้านไอทีขององค์กร แอดมินระบบจึงจำเป็นต้องระมัดระวังและใส่ใจดีไวซ์ใหม่นี้เป็นพิเศษ มีการเตรียมข้อมูลจำพวกสถานะความปลอดภัย นโยบาลและไลเซ่นซ์ไว้ล่วงหน้า เพื่อความสะดวกรวดเร็วในการใช้งานเมื่อต้องการเพิ่มดีไวซ์ใหม่เข้าระบบ
5. ตรวจสอบว่าโซลูชั่นที่ใช้อยู่ในปัจจุบันมีจำนวนไลเซ่นซ์ที่เพียงพอต่อการเพิ่มจำนวนดีไวซ์ใหม่ๆ