

# อาชีพเปิดตัว Bug Bounty โปรแกรมรายงานช่องโหว่บนเครื่องพิมพ์รายแรกในอุตสาหกรรม



ไฮไลท์ข่าว:

- อาชีพที่ร่วมมือกับบริษัทบักคราวด์ (Bugcrowd) เปิดตัว Bug Bounty สำหรับผลิตภัณฑ์เครื่องพิมพ์เป็นครั้งแรกของโลก
- อาชีพที่นำจุดยืนผู้นำเทคโนโลยีการพิมพ์ที่ปลอดภัยที่สุดในโลก เพื่อป้องกันอาชญากรรมทางไซเบอร์
- ให้เงินรางวัลสูงถึง 10,000 ดอลลาร์ หากสามารถหาช่องโหว่ของโปรแกรมนี้ได้

กรุงเทพฯ ตุลาคม 2561 – อาชีพเปิดตัว Bug Bounty โปรแกรมสำหรับรายงานช่องโหว่ด้านความปลอดภัยในเครื่องพิมพ์เป็นรายแรก เพื่อตอกย้ำจุดยืนในการส่งมอบเครื่องพิมพ์ที่มีความปลอดภัยสูงที่สุดในโลกสู่มือผู้บริโภค อาชีพที่ร่วมมือกับบักคราวด์ (Bugcrowd) บริษัทชั้นนำของโลกในด้านระบบความปลอดภัยทางไซเบอร์ เข้ามาช่วยจัดการรายงานช่องโหว่ที่อาจเป็นอันตรายต่อการใช้งาน การร่วมมือครั้งนี้เป็นการเสริมสร้างความแข็งแกร่งให้กับระบบความปลอดภัยในเครื่องพิมพ์ของ HP เพื่อประโยชน์สูงสุดของผู้ใช้

อาชีพเป็นที่ยอมรับมาอย่างยาวนานว่าเป็นผู้นำในการสร้างนวัตกรรมที่มีระบบความปลอดภัยสูง และเป็นผู้ยกระดับมาตรฐานความปลอดภัยใหม่ๆ ให้กับอุตสาหกรรม Bug Bounty โปรแกรมสำหรับเครื่องพิมพ์ของอาชีพนี้ เป็นอีกหนึ่งก้าวสำคัญในการส่งมอบความปลอดภัยระดับสูงสุดสำหรับลูกค้าและคู่ค้าของอาชีพ

“ภัยคุกคามบนโลกไซเบอร์มีความซับซ้อนและทวีขึ้นเรื่อยๆ จึงจำเป็นอย่างยิ่งที่จะต้องใช้ระบบความปลอดภัยที่น่าเชื่อถือและไวใจได้ตั้งแต่ระดับเฟิร์มแวร์ และนี่คือสิ่งที่อาชีพยึดถือในการคิดค้นพัฒนาเครื่องพิมพ์ที่มีความปลอดภัยสูงสุดของโลก” ชิวอน อัลไบรท์ หัวหน้าฝ่ายเทคโนโลยีความปลอดภัยเครื่องพิมพ์ของอาชีพ กล่าว

อาชีพเป็นบริษัทแรกที่ลงทุนในโปรแกรม Bug bounty สำหรับอุปกรณ์การพิมพ์ เพื่อส่งมอบความปลอดภัยให้ลูกค้าจากการโจมตีทางไซเบอร์ที่มีเป้าหมายทั้งทางธุรกิจและพนักงานโดยตรง จากรายงานของ Bugcrowd เมื่อเร็วๆ นี้ พบว่าเป้าหมายลำดับต้นๆ ที่กลุ่มแฮกเกอร์ให้ความสนใจโจมตีคือ อุปกรณ์ปลายทางของผู้ใช้งาน โดยอาศัยช่องโหว่ของเครื่องพิมพ์ซึ่งมีอัตราเพิ่มสูงขึ้นเรื่อยๆ ถึง 21% ในรอบปีที่ผ่านมา

จัสติน โบน CEO ของ MedSec หนึ่งในทีมที่ปรึกษาด้านความปลอดภัยทางเทคโนโลยีของอาชีพ กล่าวขำๆว่า “ถึงแม้ฝ่ายดูแลด้านความปลอดภัยสารสนเทศขององค์กร (CISO) อาจไม่ค่อยมีส่วนร่วมในการตัดสินใจจัดซื้อเครื่องพิมพ์

สำหรับองค์กรเท่าใดนัก แต่ยังคงมีบทบาทสำคัญในการดูแลความปลอดภัยและการใช้งานอุปกรณ์ต่างๆในองค์กรให้ เป็นไปอย่างปลอดภัย ราบรื่น เป็นเวลาหลายทศวรรษที่เอชพีให้ความสำคัญกับระบบรักษาความปลอดภัยทาง ไซเบอร์เป็นอันดับแรก โดยเน้นมุ่งมั่นพัฒนาเครื่องพิมพ์ที่มีระบบความปลอดภัยที่แน่นหนา ซึ่งนับเป็นการยืนหยัด ในบทบาทผู้ช่วยด้านความปลอดภัยสารสนเทศขององค์กรในทุกระดับ”

โปรแกรม Bug Bounty ที่ประกาศออกมานั้นจะมีขั้นตอนดังต่อไปนี้

- หากมีการค้นพบช่องโหว่ในโปรแกรมปฏิบัติการของบริษัท จะต้องส่งรายงานแจ้งไปยังบริษัทบั๊กคราวด์ (Bugcrowd)
- จะมีการนำไปประเมินเทียบกับรายงานช่องโหว่หรือความเสี่ยงที่เคยปรากฏก่อนหน้านี้พบโดยเอชพี และจะมอบ รางวัลให้ผู้ค้นพบช่องโหว่นั้น
- บริษัทบั๊กคราวด์ (Bugcrowd) จะทำการตรวจสอบ bugs ข้อผิดพลาดที่พบนั่นๆ และมอบรางวัลแก่ผู้พบช่องโหว่ โดยขึ้นอยู่กับระดับความรุนแรงของข้อบกพร่องที่พบโดยมีเงินรางวัลสูงสุด 10,000 ดอลลาร์

สามารถอ่านข้อมูลเพิ่มเติมสำหรับกลุ่มผลิตภัณฑ์เครื่องพิมพ์สำหรับงานธุรกิจและความปลอดภัยได้ที่:

<http://hp.com/go/printersthatprotect>