

โครงการ

“Government Cyber Safe เพื่อเฝ้าระวังและปกป้องเว็บไซต์ภาครัฐให้ปลอดภัยโฆษณาเว็บพนัน”

๑. หลักการและเหตุผล

Website Gambling เป็นการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับการฝังหรือแทรกเนื้อหาเกี่ยวกับเว็บไซต์พนันออนไลน์ ลงในเว็บไซต์ที่ถูกต้องตามกฎหมาย โดยแฮกเกอร์ใช้ช่องโหว่ของระบบเว็บไซต์เป้าหมายเพื่อเปลี่ยนแปลงเนื้อหาหรือฝังลิงก์โฆษณาการพนัน ซึ่งอาจนำไปสู่ปัญหาด้านความปลอดภัยและชื่อเสียงขององค์กรที่ได้รับผลกระทบ แฮกเกอร์อาจใช้ช่องโหว่ในเว็บไซต์ เช่น ช่องโหว่ของ WordPress, ปลั๊กอินที่ล้าสมัย หรือ SQL Injection เพื่อเข้าถึงระบบของเว็บ รวมถึงการฝังโค้ดเปลี่ยนเส้นทาง ทำให้ผู้เข้าชมเว็บไซต์เปลี่ยนเส้นทางไปยังเว็บพนันโดยอัตโนมัติ แฮกเกอร์อาจใช้มัลแวร์หรือปลั๊กอินที่ถูกบุกรุกฝังโฆษณาการพนันลงในหน้าเว็บ โฆษณาอาจล่อลวงให้ผู้เข้าชมคลิกและนำไปสู่เว็บไซต์ที่เป็นอันตราย ความเสียหายต่อชื่อเสียงของเว็บไซต์ของหน่วยงาน

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ร่วมกับมหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา (มทร.ล้านนา) ได้ดำเนินการจัดโครงการ “เว็บไซต์การศึกษาปลอดพนันออนไลน์” ให้กับหน่วยงานภาคการศึกษาในประเทศไทยเพื่อเข้าใช้งานระบบ EduShield ในการตรวจจับการโจมตีด้วยการฝังเว็บไซต์พนันออนไลน์ฯ เมื่อเดือนกรกฎาคม ๒๕๖๗ ที่ผ่านมา ซึ่งโครงการฯ ดังกล่าวได้ประสบความสำเร็จอย่างเป็นรูปธรรมในการยกระดับความปลอดภัยทางไซเบอร์ให้กับหน่วยงานภาคการศึกษาในประเทศไทย ผ่านการใช้งานระบบ EduShield ที่สามารถตรวจจับและป้องกันการโจมตีด้วยการฝังเว็บไซต์พนันออนไลน์ได้อย่างมีประสิทธิภาพ โดยผลลัพธ์ที่ได้จากการดำเนินโครงการพบว่าสถิติการตรวจพบภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับเว็บพนันออนไลน์ในหน่วยงานภาคการศึกษาที่เข้าร่วมโครงการลดลงอย่างเห็นได้ชัดเมื่อเทียบกับช่วงก่อนหน้า นอกจากนี้ ระบบ EduShield ยังช่วยลดระยะเวลาในการตอบสนองต่อเหตุการณ์จากเดิมที่อาจใช้เวลาหลายวันลงเหลือเพียงไม่กี่ชั่วโมง ส่งผลให้ความเสียหายต่อระบบและหน้าเว็บไซต์ของหน่วยงานลดน้อยลงอย่างมาก

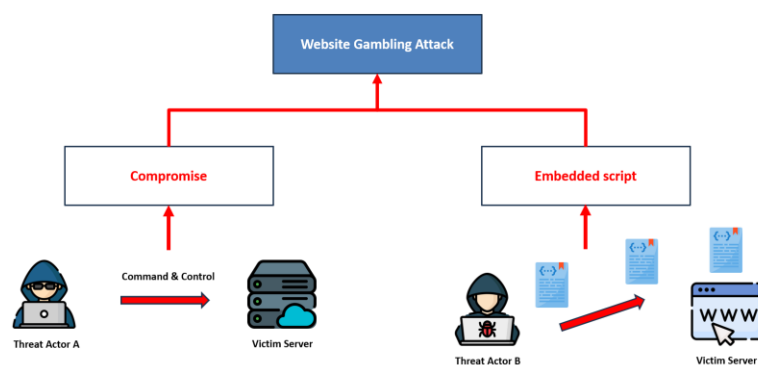
ความสำเร็จของโครงการนี้ไม่เพียงแต่ช่วยปกป้องโครงสร้างพื้นฐานดิจิทัลของหน่วยงานการศึกษาเท่านั้น แต่ยังส่งผลดีต่อภาพลักษณ์และความน่าเชื่อถือของหน่วยงานภาครัฐในสายตาของประชาชน เนื่องจากปัญหาการฝังเว็บพนันออนไลน์มักสร้างความสับสนและความไม่มั่นใจให้กับผู้ใช้งานเว็บไซต์ โดยเฉพาะนักเรียน นักศึกษาและผู้ปกครองที่เข้าใช้งานระบบการศึกษาออนไลน์ นอกจากนี้ โครงการยังได้มีการจัดอบรมบุคลากรในหน่วยงานเพื่อเพิ่มทักษะในการรับมือกับภัยคุกคามรูปแบบใหม่ ทำให้เกิดการพัฒนาศักยภาพของบุคลากรควบคู่ไปกับการใช้งานระบบ

โครงการนี้ได้กลายเป็นต้นแบบในการขยายผลไปยังหน่วยงานภาครัฐอื่น ๆ ที่ยังคงเผชิญกับปัญหาการขาดแคลนเครื่องมือตรวจจับที่มีประสิทธิภาพ ปัจจุบันพบสถิติปัญหาภัยคุกคามทางไซเบอร์ของหน่วยงานภาครัฐในประเทศไทยเป็นจำนวนมากตกเป็นเป้าหมายของการโจมตีด้วยการฝังเว็บไซต์พนันออนไลน์บนเว็บไซต์ของหน่วยงาน ทำให้หน้าเว็บไซต์หรือระบบต่าง ๆ ของหน่วยงานเกิดความเสียหาย ส่งผลกระทบต่อชื่อเสียงภาพลักษณ์ และความน่าเชื่อถือของหน่วยงานภาครัฐ

ThaiCERT ร่วมมือกับ มทร.ล้านนา พัฒนาระบบ EduShield เดิมให้กลายเป็นระบบ “Gamble Guard” ที่ได้รับการปรับปรุง เพื่อให้สามารถรองรับการใช้งานของหน่วยงานภาครัฐในหลากหลายภาคส่วน โดยมีเป้าหมายเพื่อยกระดับความปลอดภัยทางไซเบอร์ของหน่วยงานเหล่านี้ จึงได้ริเริ่มโครงการ “Government Cyber Safe เพื่อเฝ้าระวังและปกป้องเว็บไซต์ภาครัฐให้ปลอดภัยโฆษณาเว็บพนัน” โครงการนี้เชิญชวนหน่วยงานภาครัฐทั่วประเทศให้เข้ามาใช้งานระบบ Gamble Guard เพื่อตรวจจับและป้องกันการโจมตีดังกล่าว พร้อมทั้งจัดการอบรมให้แก่ผู้ดูแลเว็บไซต์ของหน่วยงาน เพื่อเสริมสร้างความรู้และความเข้าใจในการป้องกันภัยคุกคาม รวมถึงลดความเสี่ยงที่อาจเกิดขึ้นในอนาคต ซึ่งจะช่วยเสริมความแข็งแกร่งและความยั่งยืนให้กับการป้องกันภัยคุกคามทางไซเบอร์ของประเทศไทยในระยะยาว

การดำเนินการนี้ยังตอบโจทย์การยกระดับการจัดการและแก้ไขปัญหาของหน่วยงานภาครัฐอื่น ๆ ด้วย เนื่องจากปัจจุบันหลายหน่วยงานยังขาดแคลนเครื่องมือหรือระบบที่มีประสิทธิภาพในการตรวจจับและตอบสนองต่อเหตุการณ์อย่างรวดเร็ว การพัฒนาและขยายผลของระบบ Gamble Guard จึงเป็นก้าวสำคัญในการเติมเต็มช่องว่างดังกล่าวให้กับหน่วยงานภาครัฐในประเทศไทย

Website Gambling



๒. วัตถุประสงค์

- เพื่อยกระดับความปลอดภัยไซเบอร์สำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐอื่น ๆ

- เพื่อพัฒนาศักยภาพ ทักษะและความเชี่ยวชาญในการป้องกันของบุคลากรของหน่วยงาน
- เพื่อตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพให้กับผู้ดูแลเว็บไซต์ของหน่วยงาน
- เพื่อช่วยเสริมสร้างความรู้ความเข้าใจในการป้องกันและช่วยลดความเสี่ยงที่จะเกิดปัญหาขึ้นในอนาคต
- เพื่อช่วยลดงบประมาณให้กับหน่วยงานในการจัดหาเครื่องมือในการรักษาความมั่นคงปลอดภัยให้กับเว็บไซต์

๓. เป้าหมาย

- หน่วยงานควบคุมหรือกำกับดูแล
- หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- หน่วยงานภาครัฐอื่น ๆ

๔. ผลที่คาดว่าจะได้รับ

- หน่วยงานที่เข้าร่วมอบรมโครงการฯ จะได้รับการป้องกันเฝ้าระวังเว็บไซต์จากการใช้งานระบบในการตรวจจับการโจมตี สามารถตอบสนองเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ

- ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับความปลอดภัยที่เกี่ยวข้องกับภัยไซเบอร์ วิธีการ ผลกระทบ และข้อควรระวังจากภัยคุกคามทางไซเบอร์ต่างๆ ให้กับผู้ดูแลเว็บไซต์

- ผู้เข้ารับการฝึกอบรมสามารถรับมือกับภัยคุกคามและแก้ปัญหาได้อย่างถูกวิธี

๕. สิ่งที่หน่วยงานจะต้องเตรียม

- รายชื่อผู้ประสานหรือผู้ดูแลเว็บไซต์
- Domain หรือ Sub Domain ที่ต้องการใช้ในระบบ
- ข้อมูลการติดต่อของผู้ประสานงาน
- เครื่องคอมพิวเตอร์หรือแล็ปท็อปสำหรับใช้ในกิจกรรมรับชมรับฟังการบรรยายและใช้งานระบบ

ภาพประชาสัมพันธ์



FREE

GOVERNMENT CYBERSAFE

**Tuesday, March 25 2025**
09.30 - 12.00 AM





REGISTER NOW



พลอากาศตรี อมร ชนเชย
เลขาธิการคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



พันตำรวจเอก ภูมิภักดิ์ พรหมจันทร์
ผู้อำนวยการสำนักบริหารโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศ



ผู้ช่วยศาสตราจารย์
ดร.ประเสริฐ สัจใจ
ผู้อำนวยการสำนักพัฒนาระบบบริหาร
และจัดการข้อมูลสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี



นายวัชรภักดิ์ เลิศรัตนโพธิ์
เจ้าหน้าที่ ศูนย์วิจัย
เฉพาะด้านไซเบอร์



"Government Cyber Safe"

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ร่วมกับ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี จัดโครงการ "Government Cyber Safe เพื่อเฝ้าระวังและปกป้องเว็บไซต์ภาครัฐให้ปลอดภัยบนอินเทอร์เน็ต" โดยระบบเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับหน่วยงานภาครัฐโดยเฉพาะ



- ▶ รับรู้ความเสี่ยงทันที
รับข้อมูลอัปเดตเกี่ยวกับการโจมตีและการฝังเว็บมัลแวร์ออนไลน์ เพื่อให้รับมือกับภัยคุกคามได้ทันทั่วทั้ง
- ▶ ระบบตรวจจับภัยคุกคาม
ใช้เครื่องตรวจจับที่พัฒนาเฉพาะสำหรับหน่วยงานภาครัฐ
- ▶ การแจ้งเตือนเร็วทันใจ
หลังการอบรม สามารถใช้ระบบแจ้งเตือนได้ทันที เพื่อตอบสนองและปกป้องเว็บไซต์อย่างมีประสิทธิภาพ



REGISTER NOW

สอบถามข้อมูลการสมัครเพิ่มเติมได้ที่ โทร. 02-502-7845 หรือ อีเมล ncert@ncsa.or.th