คำแนะนำ

เรื่อง แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ (Website Security)

๑. เหตุผล

ปัจจุบันสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) พบการโจมตีเว็บไซต์ (Hacked Website) ของหน่วยงานต่าง ๆ ในห้วงตุลาคม ๒๕๖๔ - มีนาคม ๒๕๖๕ รวมทั้งสิ้น ๕๒ เหตุการณ์ ประกอบด้วย การพนันออนไลน์ (Gambling) จำนวน ๒๒ เหตุการณ์ เว็บไซต์ฟิชชิ่ง (Website Phishing) จำนวน ๑๗ เหตุการณ์ และการโจมตีเปลี่ยนหน้าเว็บ (Website Defacement) จำนวน ๑๓ เหตุการณ์ ส่งผลกระทบไปถึงความมั่นคงปลอดภัยของข้อมูลและความเชื่อมั่นของประชาชนในประเทศ

๒. ขอบเขต

คำแนะนำฉบับนี้ให้ใช้กับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีการจัดทำเว็บไซต์

๓. นิยาม

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๔. แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์

หัวข้อนี้ จัดทำขึ้นโดยประยุกต์ใช้หลักการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ ตาม Website Security[1] โดย Cybersecurity & Infrastructure Security Agency และ Web Security[2] จาก Mozilla เพื่อให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งมีการจัดทำ Website ของหน่วยงานสามารถมีแนวทางในการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับ Website ได้อย่างมีประสิทธิภาพ โดยมีคำแนะนำดังนี้

<u>๔.๑ ทำให้ระบบนิเวศของโดเมนมีความปลอดภัย (Secure domain ecosystems)</u>

๔.๑.๑ ตรวจสอบผู้รับจดทะเบียน (Registrar) และระเบียนระบบชื่อโดเมน (DNS records) สำหรับโดเมนทั้งหมด

๔.๑.๒ เปลี่ยนรหัสผ่านเริ่มต้นทั้งหมดที่ได้รับจากผู้รับจดทะเบียนโดเมนและ DNS ของคุณ

ชื่อผู้ใช้และรหัสผ่านเริ่มต้นไม่ปลอดภัย - โดยปกติแล้วจะสามารถค้นหาได้บนอินเทอร์เน็ต การเปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นจะป้องกันการโจมตีที่ใช้ประโยชน์จากข้อมูลดังกล่าว

๔.๑.๓ บังคับใช้การพิสูจน์และยืนยันตัวตนหลายปัจจัย (Multi-factor authentication : MFA)

๔.๑.๔ ติดตามตรวจสอบบันทึกความโปร่งใสของใบรับรอง (certificate transparency logs) เพื่อตรวจสอบเว็บไซต์ปลอมที่อาจใช้ชื่อโดเมนคล้ายกัน

<u>๔.๒ ทำให้บัญชีผู้ใช้มีความปลอดภัย (Secure user accounts)</u>

๔.๒.๑ บังคับใช้การพิสูจน์และยืนยันตัวตนหลายปัจจัยกับบัญชีผู้ใช้ทั้งหมดที่เข้าถึงได้จากอินเทอร์เน็ต โดยให้ความสำคัญกับบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged access)

๔.๒.๒ จำกัดสิทธิ์ของผู้ใช้เท่าที่จำเป็น (Principle of least privilege) รวมทั้งปิดใช้งานบัญชีและสิทธิ์ที่ไม่จำเป็น

---

[1] https://www.cisa.gov/uscert/ncas/tips/ST18-006

[2] https://infosec.mozilla.org/guidelines/web_security#web-security-cheat-sheet

๔.๒.๓ เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นทั้งหมด

๔.๓ ค้นหาและแก้ไขช่องโหว่อย่างต่อเนื่อง (Continuously scan for—and remediate -critical and high vulnerabilities)

๔.๓.๑ แก้ไขช่องโหว่ระดับวิกฤต (Critical) และระดับสูง (High) ทั้งหมด ภายใน ๑๕ และ ๓๐ วัน ตามลำดับ ในระบบที่สามารถเข้าถึงได้ทางอินเทอร์เน็ต โดยสแกนหาช่องโหว่จากการตั้งค่า (Configuration vulnerabilities) และช่องโหว่ของซอฟต์แวร์ รวมถึงเปิดใช้งานการอัปเดตอัตโนมัติทุกครั้ง

๔.๓.๒ เปลี่ยนระบบปฏิบัติการ แอปพลิเคชันและฮาร์ดแวร์ ซึ่งหมดระยะเวลาการสนับสนุนโดยผู้ผลิต

๔.๔ ทำให้ข้อมูลระหว่างการขนส่งมีความปลอดภัย (Secure data in transit)

๔.๔.๑ ปิดการใช้งาน Hypertext Transfer Protocol (HTTP); บังคับใช้ Hypertext Transfer Protocol Secure (HTTPS) และ HTTP Strict Transport Security (HSTS)

ผู้ใช้งานเว็บไซต์คาดหวังว่าความเป็นส่วนตัวของพวกเขาจะได้รับการปกป้อง ดังนั้น เพื่อให้แน่ใจว่าการสื่อสารระหว่างเว็บไซต์และผู้ใช้ได้รับการเข้ารหัส จึงต้องบังคับใช้ HTTPS เสมอ และควรบังคับใช้ HSTS หากเป็นไปได้

๔.๔.๒ ปิดการใช้งานอัลกอริทึมที่ไม่มีความมั่นคงปลอดภัย เช่น SSLv2, SSlv3, 3DES, RC4

๔.๕ สำรองข้อมูล (Backup data)

๔.๕.๑ หมั่นสำรองข้อมูลอย่างสม่ำเสมอ โดยเฉพาะข้อมูลและระบบที่สำคัญเว็บไซต์

๔.๕.๒ เก็บข้อมูลสำรองไว้ในที่ปลอดภัยและแยกทางกายภาพออกจากระบบ (Physically remote environment)

๔.๕.๓ ทดสอบการกู้คืนข้อมูล

๔.๖ ทำให้เว็บแอปพลิเคชันมีความปลอดภัย (Secure web applications)

๔.๖.๑ ระบุและลดความเสี่ยงของการถูกโจมตีบนเว็บแอปพลิเคชันที่สำคัญ ๑๐ อันดับแรก (ข้อมูลเพิ่มเติมเกี่ยวกับความเสี่ยง ๑๐ อันดับแรกจาก OWASP[3] ศึกษาเพิ่มเติมได้ที่ https://owasp.org/www-project-top-ten/) จากนั้นจึงพิจารณาระบุและลดความเสี่ยงอื่น ๆ เป็นลำดับถัดไป อาทิ การปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยของระบบและเครือข่ายที่มีการใช้งานเทคโนโลยีอินเทอร์เน็ตจาก Center for Internet Security (CIS)[4] ศึกษาเพิ่มเติมได้ที่ https://www.cisecurity.org/controls

๔.๖.๒ เปิดการบันทึกการใช้งาน (Logging) และตรวจสอบบันทึกการใช้งานกิจกรรมบนเว็บไซต์อย่างสม่ำเสมอ เพื่อตรวจหากิจกรรมที่ผิดปกติ ทั้งนี้ ควรส่งบันทึกการใช้งานดังกล่าวไปยังเซิร์ฟเวอร์ส่วนกลาง (Centralized log server)

๔.๖.๓ ใช้การพิสูจน์และยืนยันตัวตนหลายปัจจัย สำหรับผู้ใช้งาน ซึ่งล็อกอินเข้าสู่เว็บแอปพลิเคชัน รวมถึงผู้ดูแลระบบที่มีการใช้งานโครงสร้างพื้นฐานของเว็บไซต์ด้วย

๔.๗ ทำให้เว็บเซิร์ฟเวอร์มีความปลอดภัย (Secure web servers)

๔.๗.๑ ตรวจสอบความปลอดภัยโดยอ้างอิงตาม security checklist ของแอปพลิเคชันนั้น ๆ เช่น Apache, MySQL และดำเนินการตั้งค่าให้มีความมั่นคงปลอดภัย (Harden configurations)

๔.๗.๒ ใช้แอปพลิเคชันที่เชื่อถือได้และมีความจำเป็นสอดคล้องกับความต้องการขององค์กร รวมทั้งปิดการใช้งานฟีเจอร์ที่ไม่จำเป็น

---

[3] https://owasp.org/

[4] https://www.cisecurity.org/

๔.๗.๓ ใช้การแบ่งส่วนและแยกเครือข่าย (network segmentation and segregation)

- การแบ่งส่วนและแยกเครือข่ายจะทำให้ผู้โจมตีเคลื่อนไหว (Move laterally) ในเครือข่ายได้ยากขึ้น ตัวอย่างเช่น การวางเว็บเซิร์ฟเวอร์ไว้บนเครือข่ายแบบ demilitarized zone (DMZ) ที่ถูกกำหนดค่าอย่างเหมาะสมจะจำกัดการรับส่งข้อมูลที่ได้รับอนุญาตระหว่างระบบภายในเครือข่ายแบบ DMZ และระบบในเครือข่ายภายในขององค์กร

๔.๗.๔ ให้คำนึงไว้เสมอว่าทรัพย์สินอยู่ที่ไหน

- ถ้าเรารู้ว่าข้อมูลสำคัญของเราอยู่ตรงไหน เราก็จะสามารถบริหารจัดการและจำกัดการเข้าถึงได้อย่างเหมาะสม

๔.๘ จัดลำดับความสำคัญโดยใช้ Web Security Cheat Sheet

การดำเนินการเพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยนั้นสามารถดำเนินการได้หลายประการ ทั้งนี้ควรพิจารณาจากประโยชน์ที่จะได้รับ (Security Benefit) และความยากง่ายในการดำเนินการ (Implementation Difficulty) ซึ่งจะทำให้องค์กรสามารถจัดลำดับความสำคัญในการดำเนินการได้ โดยมีคำแนะนำดังปรากฏในตารางนี้

Guideline	Security Benefit	Implementation Difficulty	Ordert	Requirements	Notes
HTTPS	MAXIMUM	MEDIUM		Mandatory	Sites should HTTPS (or other secure protocols) for all communications
Public Key Pinning	LOW	MAXIMUM	--	Mandatory for maximum risk sites only	Not recommended for most sites
Redirections from HTTP	MAXIMUM	LOW	3	Mandatory	Websites must redirect to HTTPS, API endpoints should disable HTTP entirely
Resource Loading	MAXIMUM	LOW	2	Mandatory for all websites	Both passive and active resources should be loaded through protocols using TLS, such as HTTPS

Guideline	Security Benefit	Implementation Difficulty	Ordert	Requirements	Notes
Strict Transport Security	HIGH	LOW	4	Mandatory for all websites	Minimum allowed time period of six months
TLS Configuration	MEDIUM	MEDIUM	1	Mandatory	Use the most secure Mozilla TLS configuration for your user base, typically Intermediate
Content Security Policy	HIGH	HIGH	10	Mandatory for new websites Recommended for existing websites	Disabling inline script is the greatest concern for CSP implementation
Cookies	HIGH	MEDIUM	7	Mandatory for all new websites Recommended for existing websites	All cookies must be set with the Secure flag, and set as restrictively as possible
contribute.json	LOW	LOW	9	Mandatory for all new Mozilla websites Recommended for existing Mozilla sites	Mozilla sites should serve contribute.json and keep contact information up-to-date
Cross-origin Resource Sharing	HIGH	LOW	11	Mandatory	Origin sharing headers and files should not be present, except for specific use cases

Guideline	Security Benefit	Implementation Difficulty	Ordert	Requirements	Notes
Cross-site Request Forgery Tokenization	LOW	UNKNOWN	6	Varies	Mandatory for websites that allow destructive changes Unnecessary for all other websites Most application frameworks have built-in CSRF tokenization to ease implementation
Referrer Policy	LOW	LOW	12	Recommended for all websites	Improves privacy for users, prevents the leaking of internal URLs via Referer header
robots.txt	LOW	LOW	14	Optional	Websites that implement robots.txt must use it only for noted purposes
Subresource Integrity	MEDIUM	MEDIUM	15	Recommended‡	‡ Only for websites that load JavaScript or stylesheets from foreign origins
X-Content-Type-Options	LOW	LOW	8	Recommended for all websites	Websites should verify that they are setting the proper MIME types for all resources
X-Frame-Options	HIGH	LOW	5	Mandatory for all websites	Websites that don't use DENY

Guideline	Security Benefit	Implementation Difficulty	Ordert	Requirements	Notes
					or SAMEORIGIN must employ clickjacking defenses
X-XSS-Protection	LOW	MEDIUM	13	Mandatory for all new websites Recommended for existing websites	Manual testing should be done for existing websites, prior to implementation

๕. ข้อสงสัย/ข้อเสนอแนะ

หากหน่วยงานพบปัญหา ข้อขัดข้อง หรือมีความประสงค์จะเสนอแนะเพิ่มเติม เกี่ยวกับการดำเนินการตามคำแนะนำฉบับนี้ สามารถติดต่อโดยตรงได้ที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๘ โทรสาร ๐ ๒๑๔๓ ๗๕๙๓ อีเมล ncert@ncsa.or.th

๖. เรื่องอื่น ๆ

หน่วยงานสามารถติดตามข่าวสารล่าสุดจากสำนักงานผ่าน Line Openchat ตาม QR Code นี้

****