บทที่ 6

ความปลอดภัยของเว็บไซต์ (Web Security) – ฉบับลงลึก

ทำไมความปลอดภัยเว็บไซต์ถึงสำคัญ?

หน้าร้านดิจิทัล

เว็บไซต์คือหน้าร้านดิจิทัลที่ต้องปกป้องข้อมูลลูกค้าและธุรกิจอันมีค่า

ภัยคุกคามที่เพิ่มขึ้น

การโจมตีเว็บเซิร์ฟเวอร์เพิ่มขึ้น 30% ในไทยในปี 2025 (ที่มา: ThaiCERT)

ความเสียหายมหาศาล

ความเสียหายจากข้อมูลรั่วไหลอาจสูงถึงหลักล้านบาทต่อเหตุการณ์ครั้งเดียว

ภัยคุกคามหลักที่เว็บไซต์ต้องเผชิญ

SQL Injection

แฮกเกอร์เจาะฐานข้อมูลผ่านช่องโหว่ในฟอร์มป้อนข้อมูล

Cross-Site Scripting (XSS)

การฝังโค้ดอันตรายบนเว็บเพื่อขโมยข้อมูลของผู้ใช้งาน

Session Hijacking

ขโมยสิทธิ์ผู้ใช้เพื่อเข้าถึงข้อมูลส่วนตัวและดำเนินการในนามของเขา

CSRF

การปลอมคำสั่งจากผู้ใช้โดยที่ผู้ใช้ไม่รู้ตัว ก่อให้เกิดความเสียหายได้

มาตรฐานความปลอดภัยเว็บไซต์ในไทย

- **ข้อเสนอแนะมาตรฐาน ETDA (2557):** เน้นการรักษาความปลอดภัยในหลายส่วน ได้แก่ Web Server, CMS, Database และ Web Application

- **อ้างอิงมาตรฐานสากล:** โดยมีการอ้างอิงและปรับใช้ตามมาตรฐานระดับโลก เช่น NIST, OWASP และ IPA Japan
- **ISO/IEC 27001-2566:** มาตรฐานสากลสำหรับการจัดการระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นสิ่งสำคัญสำหรับองค์กร

แนวทางปฏิบัติการตั้งค่าเว็บเซิร์ฟเวอร์อย่างมั่นคงปลอดภัย

กำหนดค่า Firewall

ปฏิเสธการเชื่อมต่อที่ไม่จำเป็น เพื่อลดความเสี่ยงจากการโจมตี

จำกัดสิทธิ์ผู้ดูแลระบบ

จำกัดสิทธิ์ผู้ดูแลระบบ (Admin) อย่างเข้มงวด เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

ตั้งค่ารหัสผ่านซับซ้อน

ใช้รหัสผ่านที่ซับซ้อนและเปลี่ยนรหัสผ่านทุก 2 เดือนเพื่อความปลอดภัย

สำรองและบันทึกข้อมูล

สำรองข้อมูลและบันทึกข้อมูลจราจรเครือข่ายอย่างน้อย 90 วัน เพื่อการตรวจสอบย้อนหลัง

การพัฒนาเว็บแอปพลิเคชันที่ปลอดภัย

ป้องกัน SQL Injection

ใช้ Prepared Statements เพื่อหลีกเลี่ยงการโจมตีฐานข้อมูล

ตรวจสอบข้อมูลผู้ใช้

กรองข้อมูลผู้ใช้ทุกครั้งก่อนประมวลผล เพื่อความปลอดภัยของระบบ

ใช้ Content Security Policy (CSP)

ลดความเสี่ยง XSS ด้วยการควบคุมแหล่งที่มาของเนื้อหา

ป้องกัน CSRF ด้วย Token

ตรวจสอบแหล่งที่มาของคำขอ เพื่อป้องกันการปลอมแปลง

การบริหารจัดการและรับมือเหตุการณ์โจมตีเว็บไซต์

ทีมตรวจสอบ 24 ชม.

มีทีมงานดูแลและตรวจสอบเว็บไซต์ตลอดเวลา

สแกนช่องโหว่

ใช้โปรแกรมสแกนหาช่องโหว่และตรวจจับพฤติกรรมที่ผิดปกติ

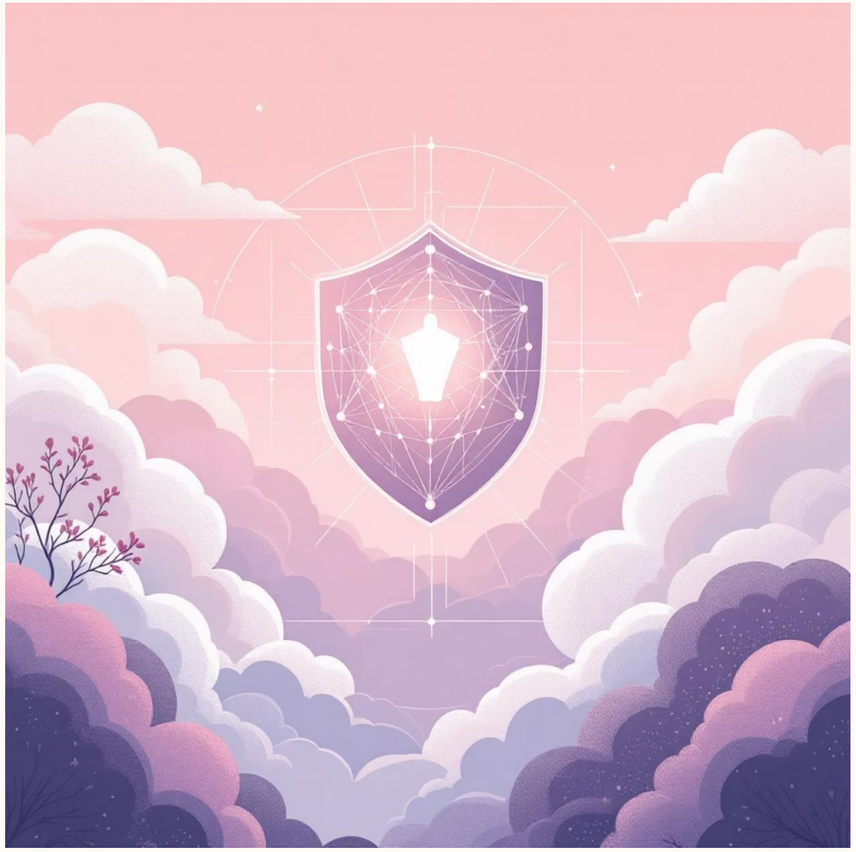
แผนกู้คืนฉุกเฉิน

มีแผนสำรองข้อมูลและระบบกู้คืนฉุกเฉิน (DR)

รายงานเหตุการณ์

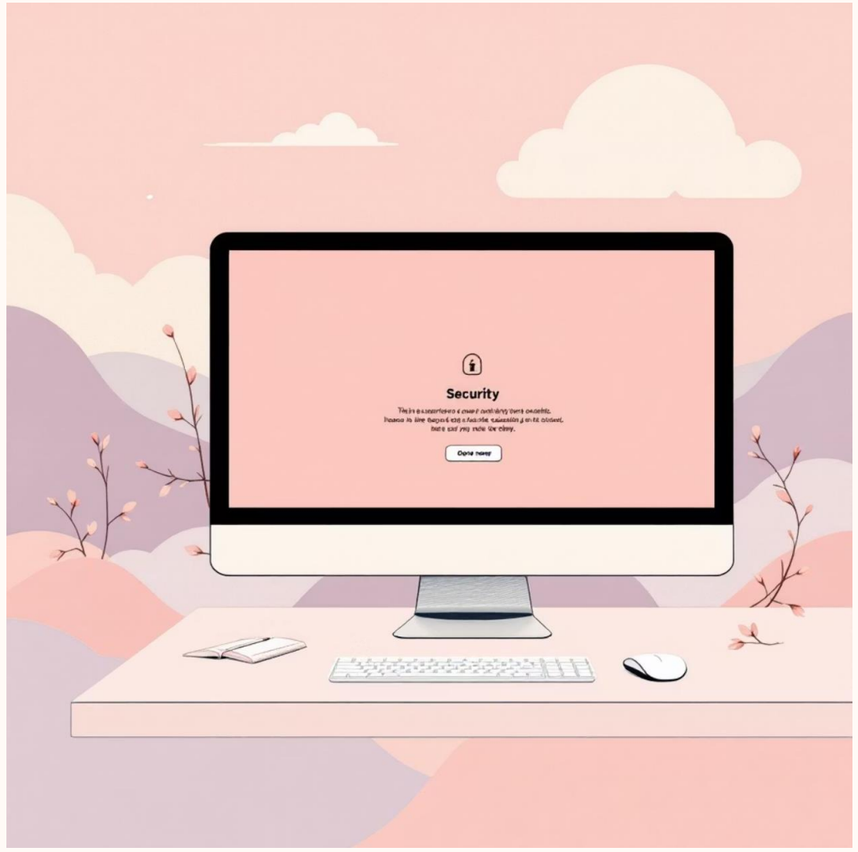
รายงานและแจ้งเตือนเหตุการณ์ทันที พร้อมมาตรการแก้ไข

กรณีศึกษาความสำเร็จและบทเรียนจากไทย



การใช้ Firewall และ DMZ

จังหวัดหนึ่งใช้ระบบ Firewall และ DMZ ป้องกันการโจมตีได้สำเร็จ แสดงให้เห็นถึงประสิทธิภาพของมาตรการเชิงรุก



อัปเดต CMS และแพตช์ระบบ

การอัปเดต CMS และแพตช์ระบบอย่างสม่ำเสมอ สามารถลดช่องโหว่ได้ถึง 85% ซึ่งเป็นปัจจัยสำคัญในการรักษาความปลอดภัย

การฝึกอบรมผู้ดูแลระบบยังช่วยลดความผิดพลาดจากมนุษย์และเพิ่มความปลอดภัยโดยรวมของระบบได้อย่างมีนัยสำคัญ

บทบาทขององค์กรและผู้ดูแลเว็บไซต์

1

นโยบายความปลอดภัย

กำหนดนโยบายความปลอดภัยอย่างชัดเจนและสื่อสารสู่ทีมงานทุกคน

2

วัฒนธรรมไซเบอร์

สร้างวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กรให้แข็งแกร่ง

3

ติดตามภัยคุกคาม

ติดตามและปรับปรุงมาตรการตามเทคโนโลยีและภัยคุกคามใหม่ๆ อยู่เสมอ

4

ร่วมมือกับภาครัฐ

ร่วมมือกับหน่วยงานภาครัฐ เช่น ETDA, ThaiCERT เพื่อรับข้อมูลและคำแนะนำที่เป็นประโยชน์

สรุปและเชิญชวนลงมือทำ

หัวใจของธุรกิจ

ความปลอดภัยเว็บไซต์คือหัวใจสำคัญของความน่าเชื่อถือและความยั่งยืนทางธุรกิจในยุคดิจิทัล

เริ่มต้นวันนี้

เริ่มต้นจากมาตรฐานและแนวทางปฏิบัติที่ถูกต้อง พร้อมติดตามภัยคุกคามอย่างใกล้ชิด

ปกป้องอนาคต

ลงมือป้องกันวันนี้ เพื่อปกป้องข้อมูลและความสำเร็จขององค์กรในอนาคต

> **“ปลอดภัยวันนี้ เพื่ออนาคตที่มั่นคงของเว็บไซต์คุณ”**