บทที่ 4 ภัยคุกคามจากการใช้งานทางอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ตถือได้ว่าเป็นภัยอันตรายต่อสังคมในปัจจุบันเป็นอย่างมาก เพราะนอกจากภัยนี้จะเป็นการรบกวนการทำงานของผู้ที่ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตแล้ว ยังส่งผลเสียต่อข้อมูลสำคัญๆ ที่มีอยู่ ชนิดของภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต จำแนกได้ดังนี้

1. มัลแวร์ (Malware) คือความไม่ปกติทางโปรแกรมที่สูญเสียความลับทางข้อมูล (Confidentiality) ข้อมูลถูกเปลี่ยนแปลง (Integrity) สูญเสียเสถียรภาพของระบบปฏิบัติการ (Availability) ซึ่งมัลแวร์แบ่งออกได้เป็นหลายประเภท ดังนี้

1.1 ไวรัสคอมพิวเตอร์ (Computer Virus) คือ รหัสหรือโปรแกรมที่สามารถทำสำเนาตัวเองและแพร่กระจายสู่เครื่องอื่นได้ โดยเจ้าของเครื่องนั้นๆ ไม่รู้ตัว ถือว่าเป็นสิ่งไม่พึงประสงค์ซึ่งฝังตัวเองในโปรแกรมหรือไฟล์ แล้วแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ ผ่านทางสื่อต่างๆ สิ่งสำคัญคือไวรัสไม่สามารถแพร่กระจายได้หากขาดคนกระทำ เช่น แบ่งปันไฟล์ที่ติดไวรัสหรือส่งอีเมล์ที่ติดไวรัสเป็นต้น

1.2 หนอนคอมพิวเตอร์ (Computer Worm) เรียกสั้นๆ ว่า เวิร์ม เป็นหน่วยย่อยลงมาจากไวรัส มีคุณสมบัติต่างๆ เหมือนไวรัสแต่ต่างกันที่เวิร์มไม่ต้องอาศัยผู้ใช้งาน แต่จะอาศัยไฟล์หรือคุณสมบัติในการส่งต่อข้อมูลในคอมพิวเตอร์เพื่อกระจายตัวเอง บางทีเวิร์มสามารถติดตั้ง Backdoor ที่เริ่มติดเวิร์มและสร้างสำเนาตัวเองได้ ซึ่งผู้สร้างเวิร์มนั้นสามารถสั่งการได้จากระยะไกล ที่เรียกว่า Botnet โดยมีเป้าหมายเพื่อโจมตีคอมพิวเตอร์และเครือข่าย ส่งที่อันตรายอย่างยิ่งของเวิร์มคือ สามารถจำลองตัวเองในคอมพิวเตอร์เครื่องหนึ่งแล้วแพร่กระจายตัวเองออกไปได้จำนวนมาก ตัวอย่างเช่น สามารถดักจับ username และ password และใช้ข้อมูลนี้เพื่อบุกรุกบัญชีผู้ใช้นั้น ทำสำเนาตัวเองแล้วส่งต่อไปยังทุกรายชื่อที่มีอยู่ในลิสต์อีเมล และเมื่อสำเนาตัวเองเป็นจำนวนมากจะทำให้การส่งข้อมูลผ่านเครือข่ายช้าลง เป็นเหตุให้ Web Server และเครื่องคอมพิวเตอร์หยุดทำงาน

1.3 ม้าโทรจัน (Trojan Horse) คือ โปรแกรมชนิดหนึ่งที่ดูเหมือนมีประโยชน์ แต่แท้ที่จริงก่อให้เกิดความเสียหายเมื่อรันโปรแกรม หรือติดตั้งบนคอมพิวเตอร์ ผู้ที่ได้รับไฟล์โทรจันมักถูกหลอกลวงให้เปิดไฟล์ดังกล่าว โดยหลงคิดว่าเป็นซอฟต์แวร์ถูกกฎหมาย หรือไฟล์จากแหล่งที่ถูกต้องตามกฎหมาย เมื่อไฟล์ถูกเปิดอาจส่งผลลัพธ์หลายรูปแบบ เช่น สร้างความรำคาญด้วยการเปลี่ยนหน้าจอ สร้างไอคอนที่ไม่จำเป็น จนถึงขั้นลบไฟล์และทำลายข้อมูล โทรจันต่างจากไวรัสและเวิร์มคือโทรจันไม่สามารถสร้างสำเนาโดยแพร่กระจายสู่ไฟล์อื่น และไม่สามารถจำลองตัวเองได้

1.4 Backdoor แปลเป็นไทยก็คือประตูหลัง ที่เปิดทิ้งไว้ให้บุคคลอื่นเดินเข้านอกออกในบ้านได้โดยง่าย ซึ่งเป็นช่องทางลัดที่เกิดจากช่องโหว่ของระบบ ทำให้ผู้ไม่มีสิทธิเข้าถึงระบบหรือเครื่องคอมพิวเตอร์เพื่อทำการใดๆ

1.5 สปายแวร์ (Spyware) คือ มัลแวร์ชนิดหนึ่งที่ติดตั้งบนเครื่องคอมพิวเตอร์แล้วทำให้ล่วงรู้ข้อมูลของผู้ใช้งานได้โดยเจ้าของเครื่องไม่รู้ตัว สามารถเฝ้าดูการใช้งานและรวบรวมข้อมูลส่วนตัวของผู้ใช้ได้ เช่น นิสัยการท่องอินเทอร์เน็ต และเว็บไซต์ที่เข้าชม ทั้งยังสามารถเปลี่ยนค่าที่ตั้งไว้ของคอมพิวเตอร์ ส่งผลให้ความเร็วในการเชื่อมต่ออินเทอร์เน็ตช้าลง เป็นต้น สายแวร์ที่มีชื่อคุ้นเคยกันดีคือโปรแกรม Keylogger ซึ่งตกเป็นข่าวหน้าหนึ่งของหนังสือพิมพ์ เมื่อผู้ใช้ดาวน์โหลดไฟล์จากอินเทอร์เน็ตที่แฝงโปรแกรมนี้ จะทำให้โปรแกรมเข้าฝังตัวในคอมพิวเตอร์ส่วนตัว เมื่อผู้ใช้คอมพิวเตอร์ทำธุรกรรมการเงินทางอินเทอร์เน็ต ข้อมูล username และ password ของบัญชีผู้ใช้จึงถูกส่งตรงถึงมิจฉาชีพ และลักลอบโอนเงินออกมาโดยเจ้าของตัวจริงไม่รู้ตัว เป็นต้น

2. การโจมตีแบบ DoS/DDos คือการพยายามโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน หรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง(ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน จะเรียกกว่าการโจมตีแบบ Distributed Denial of Service (DDoS) ซึ่งในปัจจุบันการโจมตีส่วนใหญ่มักเป็นการโจมตีแบบ DDoS

3. BOTNET หรือ “Robot network” คือเครือข่ายหุ่นรบที่ถือเป็นสะพานเชื่อมภัยคุกคามทางเครือข่ายคอมพิวเตอร์ ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้นต้องการนำทางเพื่อต่อยอดความเสียหายและทำให้ยากแต่การควบคุมมากขึ้น

4. ข้อมูลขยะ (Spam) คือ ภัยคุกคามส่วนใหญ่ที่เกิดจากอีเมลหรือเรียกว่า อีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti-spam หรือใช้บริการคัดกรองอีเมลของเว็บไซต์ที่ให้บริการอีเมล หลายคนอาจจะสงสัยว่า spammer รู้อีเมลเราได้อย่างไร คำตอบคือได้จากเว็บไซต์ ห้องสนทนา ลิสต์รายชื่อลูกค้า รวมทั้งไวรัสชนิดต่างๆ ที่เป็นแหล่งรวบรวมอีเมลและถูกส่งต่อกันไปเป็นทอดๆ ซึ่งหากจำเป็นต้องเผยแพร่อีเมลทางอินเทอร์เน็ตโดยป้องกันการถูกค้นเจอจาก Botnet สามารถทำได้โดยเปลี่ยนวิธีการสะกดโดยเปลี่ยนจาก “@” เป็น “at” แทน

5. Phishing เป็นคำพ้องเสียงกับ “fishing” หรือการตกปลาเพื่อให้เหยื่อมาติดเบ็ด คือ กลลวงชนิดหนึ่งในโลกไซเบอร์ด้วยการส่งข้อมูลผ่านอีเมลหรือเมสเซนเจอร์ หลอกให้เหยื่อหลงเชื่อว่าเป็นสถาบันการเงินหรือองค์กรน่าเชื่อถือ แล้วทำลิงค์ล่อให้เหยื่อคลิก เพื่อหวังจะได้ข้อมูลสำคัญ เช่น username/password, เลขที่บัญชีธนาคาร, เลขที่บัตรเครดิต เป็นต้น แต่ลิงค์ดังกล่าวถูกนำไปสู่หน้าเว็บเลียนแบบ หากเหยื่อเผลอกรอกข้อมูลส่วนตัวลงไป มิจฉาชีพสามารถนำข้อมูลไปหาประโยชน์ในทางมิชอบได้

6. Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งบนเครือข่ายในองค์กร (LAN) เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้ดักข้อมูลเพื่อแกะรหัสผ่านบนเครือข่ายไร้สาย (Wirdless LAN) และดักข้อมูล User/Password ของผู้อื่นที่ไม่ได้ผ่านการเข้ารหัส [1]

4.1 วิธีสังเกตภัยคุกคามจากอินเทอร์เน็ต

ปัจจุบันการขยายตัวของเครือข่ายออนไลน์เป็นไปอย่างรวดเร็วและเติบโตอย่างกว้างขวางจนเรียกได้ว่ากลายเป็นศูนย์รวมสินค้าขนาดมหึมา สำหรับกลุ่มนักล่าออนไลน์ที่มุ่งจะล่วงละเมิดทางเพศต่อเยาว ชน เว็บไซต์ประเภทต่างๆ ไม่ว่าจะเป็นไดอารี่ออนไลน์ เว็บหาเพื่อนร่วมโรงเรียนหรือต่างโรงเรียน เว็บหาคู่ ที่เรียก ว่าชุมชนออนไลน์ หรือการเล่นแชทไลน์ 1900 กลายเป็นสื่อร้ายที่ผู้กระทำผิดคิดมิชอบต่อเยาวชน ผู้อ่อนด้อยต่อโลก เข้าไปค้นหาข้อมูลแล้วกระทำการล่อลวง เยาวชนของเราให้กลายเป็นเหยื่อชั้นดีอย่างง่ายดาย ตามข่าวเศร้าที่ได้พบ เห็นจากสื่อต่างๆ ทั้ง TV และ หนังสือพิมพ์ เหตุเพราะเยาวชนของเราหลงไปติดกับดัก โพสต์ข้อมูลส่วนตัว วิธีการติดต่อผ่าน mail และโปรแกรมรูปแบบต่างๆ

4.1.1 แนวทางการรับมือกับภัยออนไลน์

1) เมื่อตัวเราเอง หรือบุคคลใกล้ชิด ใช้เวลาเล่น Net มากเกินจำเป็น โดยเฉพาะช่วงเย็นถึงดึก และมักมีพิรุธปิดหน้าจอหรือเปลี่ยนหน้าจอทันทีที่ท่านเดินผ่าน

2) เมื่อพบว่าได้มีการ down load ภาพลามกไว้ใน computer ซึ่งได้รับจากนักล่าออนไลน์ส่งมากระตุ้นเร้าความรู้สึก และสร้างความคุ้นเคยทางเพศให้ผู้รับภาพ

3) เมื่อพบว่าตัวเอง หรือบุคคลใกล้ชิด ได้รับโทรศัพท์ จากบุคคลที่ไม่เคยรู้จักมาก่อนหรือมีการใช้โทรศัพท์ทางไกลไปยังหมายเลขที่ไม่รู้จัก

4) เมื่อมีพัสดุ ของขวัญ จดหมายลึกลับมาให้ตัวเรา หรือบุคคลใกล้ชิดของท่าน

5) เมื่อตัวเรา หรือบุคคลใกล้ชิด มีอาการห่างเหินกับกิจกรรมของสมาชิกในครอบครัวแยกตัวจากกลุ่ม หรือเก็บตัวอยู่คนเดียว [2]

4.1.2 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต

1) การตั้งสติก่อนเปิดเครื่อง ต้องรู้ตัวก่อนเสมอว่าเราอยู่ที่ไหน ที่นั่นปลอดภัยเพียงใด

2) ก่อน login เข้าใช้งานคอมพิวเตอร์ต้องมั่นใจว่าไม่มีใครแอบดูรหัสผ่านของเรา

3) เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ ควรล็อกหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า login

4) ตระหนักอยู่เสมอว่าข้อมูลความลับและความเป็นส่วนตัวอาจถูกเปิดเผยได้เสมอในโลกออนไลน์

5) การกำหนด password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้นและการใช้งานอินเทอร์เน็ตทั่วไป เช่นการ Login ระบบ e-mail, ระบบสนทนาออนไลน์ (chat), ระบบเว็บไซต์ที่เป็นสมาชิกอยู่ ทางที่ดีควรใช้ password ที่ต่างกันบ้างพอให้จำได้

6) การสังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์ถูกเรียกใช้ขึ้นมาพร้อมๆ กับการเปิด

เครื่องหรือไม่ ถ้าสังเกตไม่ทันให้สังเกตระยะเวลาบูธเครื่อง หากนานผิดปกติอาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรือภัยคุกคามรูปแบบต่างๆ ได้

7) การหมั่นตรวจสอบและอัพเดท OS หรือซอฟต์แวร์ที่ใช้ให้เป็นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่องคอมพิวเตอร์ เช่น โปรแกรมป้องกันไวรัส, โปรแกรมไฟร์วอลล์ และควรใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย นอกจากนี้ควรอัพเดทอินเทอร์เน็ตเบราเซอร์ให้ทันสมัยอยู่เสมอ

8) ไม่ลงซอฟต์แวร์มากเกินความจำเป็น

<u>ซอฟต์แวร์ที่จำเป็นต้องลงในเครื่องคอมพิวเตอร์</u> ได้แก่

- อินเทอร์เน็ตเบราเซอร์ เพื่อให้เปิดเว็บไซต์ต่างๆ
- อีเมลเพื่อใช้รับส่งข้อมูลและติดต่อสื่อสาร
- โปรแกรมสำหรับงานด้านเอกสาร, โปรแกรมตกแต่งภาพ เสียง วีดีโอ
- โปรแกรมป้องกันไวรัสคอมพิวเตอร์และโปรแกรมไฟร์วอลล์

<u>ซอฟต์แวร์ที่ไม่ควรมีบนเครื่องคอมพิวเตอร์ที่ใช้งาน</u> ได้แก่

- ซอฟต์แวร์ที่ใช้ในการ Crack โปรแกรม
- ซอฟต์แวร์สำเร็จรูปที่ใช้ในการโจมตีระบบ, เจาะระบบ (Hacking Tools)
- โปรแกรมที่เกี่ยวกับการสแกนข้อมูล การดักรับข้อมูล (Sniffer) และอื่นๆ ที่อยู่ในรูปซอฟต์แวร์สำเร็จรูปที่ไม่เป็นที่รู้จัก
- ซอฟต์แวร์ที่ใช้หลบหลีกการป้องกัน เช่น โปรแกรมซ่อน IP Address

9) ไม่ควรเข้าเว็บไซต์เสี่ยงภัยเว็บไซต์ประเภทนี้ ได้แก่

- เว็บไซต์ลามก อนาจาร
- เว็บไซต์การพนัน
- เว็บไซต์ที่มีหัวเรื่อง “Free” แม้กระทั่ง Free Wi-Fi
- เว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมที่มีการแนบไฟล์พร้อมทำงานในเครื่องคอมพิวเตอร์
- เว็บไซต์ที่แจก Serial Number เพื่อใช้ Crack โปรแกรม
- เว็บไซต์ที่ให้ดาวน์โหลดเครื่องมือในการเจาะระบบ

10) สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์ เว็บไซต์ E-Commerce ที่ปลอดภัยควรมีการทำ HTTPS มีใบรับรองทางอิเล็กทรอนิกส์ และมีมาตรฐานรองรับ

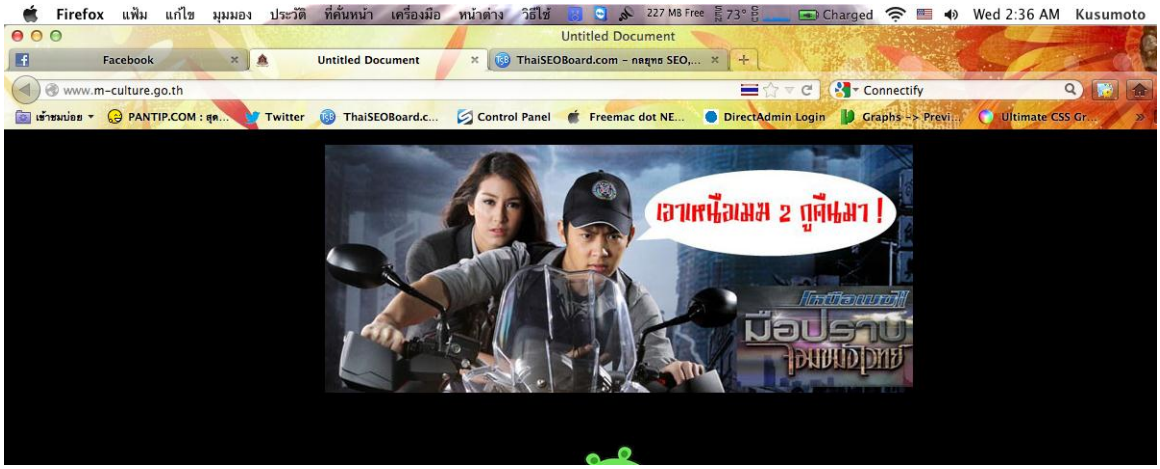
11) ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network ชื่อที่ใช้ควรเป็นชื่อเล่นหรือฉายาที่กลุ่มเพื่อนรู้จัก และไม่ควรเปิดเผยข้อมูลดังต่อไปนี้ เลขที่บัตรประชาชน เบอร์โทรศัพท์ หมายเลขบัตรเครดิต หมายเลขหนังสือเดินทาง ข้อมูลทางการแพทย์ ประวัติการทำงาน

12) ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเทอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีหลักการง่ายๆ ที่จะช่วยให้สังคมออนไลน์สงบสุข คือให้คำนึงถึงใจเขาใจเรา

13) ไม่หลงเชื่อโดยง่าย อย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเทอร์เน็ต ควรหมั่นศึกษาหาความรู้จากเทคโนโลยีอินเทอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนปักใจเชื่อในสิ่งที่ได้รับรู้

4.2 กรณีศึกษาเกี่ยวกับภัยคุกคามจากการใช้งานทางอินเทอร์เน็ต

แฮกเว็บกระทรวงวัฒนธรรม



รูปที่ 3-35 ตัวอย่างเว็บไซต์ที่ถูกแอกระบบข้อมูล

เว็บไซต์ของกระทรวงวัฒนธรรม (www.m-culture.go.th) ถูกแฮกระบบข้อมูล มีการนำลิงค์เว็บไซต์พนันบอลมาโพสต์ไว้ มีแฮกเกอร์ ใช้ชื่อว่า THE BAD PIGGIES TEAM โดยโพสต์ภาพละครเหนือเมฆ 2 โดยมีข้อความระบุว่า “เอาเหนือเมฆ 2 กูคืนมา”

จากการระงับการถ่ายทอดละครหลังข่าวทางโทรทัศน์ เข้าใจว่าอาจเป็นการแสดงให้เห็นถึง การจำกัดสิทธิในการแสดงออกทางความคิด และส่งผลให้เกิดกลุ่มบุคคลที่ไม่พึงพอใจกับการกระทำนี้ ถึงแม้ว่าการแฮกเข้าเว็บของกระทรวงวัฒนธรรม กระทำเพื่อเรียกร้องสิทธิเสรีภาพในการแสดงออกทางความคิด แต่ก็ก่อให้เกิดความเสียหายต่อข้อมูล และชื่อเสียงของกระทรวงวัฒนธรรม ที่เป็นหน่วยงานระดับประเทศนั้น เป็นการกระทำที่ผิด ไม่สมควรที่จะกระทำ เพราะยังมีวิธีการแสดงความคิดในแบบอื่นๆอีกหลายวิธี โดยที่จะไม่ก่อให้เกิดความเสียหายในด้านอื่นๆ และการกระทำนี้จะส่งผลในทางเสียหายอื่นๆอีกมาก เช่น การถูกมองว่าเป็นหน่วยงานระดับประเทศแต่มีการป้องกันระบบสารสนเทศที่ไม่มีความปลอดภัย ข้อมูลใดๆที่สำคัญหรือเป็นความลับก็มีความเสี่ยง และไม่ปลอดภัยมาก ขาดความน่าเชื่อถือ เป็นต้น อีกทั้งการกระทำในลักษณะนี้ยังเป็นการกระทำผิดกฎหมายเกี่ยวกับคอมพิวเตอร์ ในการก่อความเสียหายให้กับเว็บไซต์ โดยการเข้าระบบที่ผู้อื่นมีการป้องกันและก่อความเสียหายทางข้อมูล ซึ่งการแสดงออกทางความคิดอาจไม่ผิดในแง่จริยธรรม แต่การคุกคามระบบที่มีการป้องกันก็ไม่ใช้การกระทำที่มีความประสงค์ที่ดีแน่นอน

สาเหตุของปัญหาเกิดจากความไม่พอใจในเรื่องส่วนบุคคล ที่เกิดจากการระงับการถ่ายทอดละครหลังข่าวทางโทรทัศน์ ของกลุ่มบุคคลที่ไม่ประสงค์ดี

ผู้มีส่วนรับผิดชอบ ได้แก่ เจ้าหน้าที่ผู้ดูแลเว็บไซต์ของกระทรวงวัฒนธรรม, กลุ่มบุคคลที่ทำการแฮกเว็บไซต์ให้เกิดความเสียหาย, ผู้บริการด้านสารสนเทศ และผู้บริหารระดับสูงของกระทรวงวัฒนธรรม

วิธีการแก้ปัญหา ได้แก่ เพิ่มนโยบาย มาตรการต่างๆให้ระบบสารสนเทศมีความแข็งแรง เช่น การกำหนดระยะเวลาในการเปลี่ยนพาสเวิร์ดของการเข้าถึงข้อมูลสำคัญ หาข้อบกพร่อง ช่องโหว่จากความเสียหายครั้งนี้และพัฒนาระบบเพื่ออุดช่องโหว่ และป้องกันเว็บไซต์ เช่น การนำระบบสมาชิก เพื่อทำการยืนยันบุคคล

มีการตรวจสอบ และเก็บข้อมูลการเข้าถึง เพื่อสังเกตกลุ่มบุคคลที่เข้าข่ายเสี่ยง หรือมีพฤติกรรมที่น่าสงสัยในการเข้าเว็บไซต์ [3]

บรรณนานุกรมประจำบทที่ 4

[1] http://www.nattapon.com/2011/12/%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%84%E0%B8%B8%E0%B8%81%E0%B8%84%E0%B8%B2%E0%B8%A1%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%AD%E0%B8%B4%E0%B8%99%E0%B9%80%E0%B8%97%E0%B8%AD%E0%B8%A3%E0%B9%8C%E0%B9%80%E0%B8%99/ (สืบค้นเมื่อวันที่ 23 สิงหาคม 2556)

[2] http://www.dkt.ac.th/kruya/50webm6/unit1/internet/page7.htm (สืบค้นเมื่อวันที่ 23 สิงหาคม 2556)

[3] http://news.mthai.com/general-news/213055.html (สืบค้นเมื่อวันที่ 23 สิงหาคม 2556)