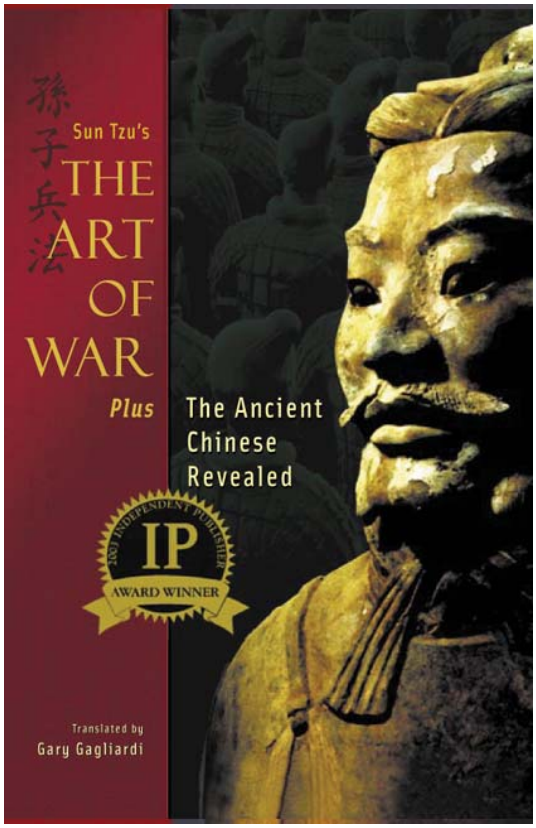
ภัยคุกคามความมั่นคงระบบสารสนเทศ

“ ภัยคุกคามที่ยิ่งใหญ่แห่งศตวรรษที่เพิ่งเริ่มต้น ที่น้อยคนจะเชื่อ ”

ประมาณ 500 ปี ก่อนคริตศักราช ชาวจีนชื่อ ซัน ซุน วู ได้เขียนเรื่อง Art of war ให้ความสำคัญกับการรู้จักตัวเองรวมถึงภัยคุกคามที่ต้องเผชิญ เพื่อจะได้รู้ว่าควรปกป้องข้อมูลขององค์กรอย่างไร



พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ

นายทหารฝ่ายเสนาธิการประจำรองผู้บัญชาการทหารสูงสุด กองทัพไทย

คณะกรรมการกำหนดและจัดสรรคลื่นความถี่ใหม่ และ คณะกรรมการประสานงานการบริหารคลื่นความถี่เพื่อความมั่นคงของรัฐ ในคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

ประธานที่ปรึกษาโครงการการบริหารคลื่นความถี่ด้วยเทคโนโลยีใหม่

สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

คำนำ

ปัจจุบันอินเตอร์เน็ตมีความสำคัญต่อการดำเนินกิจกรรมต่างๆ ทั้งการใช้งานส่วนตัว การดำเนินงานทั้งภาครัฐและเอกชน โดยเฉพาะอย่างยิ่งองค์กรที่ต้องการเชื่อมต่อเครือข่ายภายในกับเครือข่ายภายนอก เพื่อที่จะได้รับประโยชน์จากการทำธุรกรรมต่างๆ ย่อมมีความเสี่ยงจากภัยคุกคาม ดั้งนั้นองค์กรควรให้ความสำคัญกับการป้องกันความปลอดภัยของข้อมูล และระบบสารสนเทศให้มั่นคงปลอดภัยจากการโจมตีระบบ ซึ่งพนักงานทุกคนต้องตระหนึกถึงความสำคัญ และร่วมมือปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูล จึงจะเกิดระบบที่มีประสิทธิภาพ

ผู้เขียนขอขอบคุณลูกศิษย์ หลักสูตรปริญญาโทสาขาบริหารเทคโนโลยีสารสนเทศ (MSITM) มหาวิทยาลัยกรุงเทพ ที่ช่วยรวบรวมข้อมูล ความดีของผลงานนี้ขอมอบให้ลูกศิษย์ ส่วนข้อผิดพลาดอาจารย์ขอรับไว้เอง

พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ

29 กรกฎาคม 2552

สารบัญ

หน้า

สารบัญตาราง

สารบัญรูปภาพ

- - - - - - - - - - - -

ประวัติ พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ (นตท.26, จปร.37)

Mobile: 081-870-9621 settapong_m@hotmail.com

ปัจจุบันปฏิบัติหน้าที่ในตำแหน่ง นายทหารฝ่ายเสนาธิการประจำรองผู้บัญชาการทหารสูงสุด (ทบ.) กองบัญชาการกองทัพไทย, อาจารย์พิเศษโรงเรียนนายร้อยพระจุลจอมเกล้า, คณะทำงาน Next Generation Network (NGN) Forum และกองบรรณาธิการ NGN Forum กทช., ประธานที่ปรึกษาโครงการการจัดสรรคลื่นความถี่แบบ Dynamic Spectrum Allocation คณะกรรมการกิจการโทรคมนาคมแห่งชาติ, คณะกรรมการกำหนดและจัดสรรคลื่นความถี่ใหม่ กทช. และ Associate Professor of Southern New Hampshire University และ American University of London (Distance Learning Program), USA.

จบการศึกษาปริญญาตรีด้านวิศวกรรมไฟฟ้าสื่อสารโทรคมนาคมจากโรงเรียนนายร้อยพระจุลจอมเกล้า (เกียรตินิยมเหรียญทอง) ปริญญาโทและเอก (เกียรตินิยมจาก Tau Beta Pi Engineering Honor Society, USA) ด้านวิศวกรรมไฟฟ้าสื่อสารโทรคมนาคมจาก Georgia Institute of Technology และ State University System of Florida (Florida Atlantic University) ประเทศสหรัฐอเมริกา ตามลำดับ โดยทุนกองทัพไทย จบการศึกษาหลักสูตรเสนาธิการทหารบก ในระหว่างรับราชการในกองบัญชาการกองทัพไทยได้รับคัดเลือกจากกระทรวงกลาโหมสหรัฐอเมริกา เพื่อเข้ารับการฝึกอบรมในหลักสูตรต่อต้านก่อการร้ายสากล (Joint and Combined Warfighting School, Counter Terrorism Fellowship Program) ที่ National Defense University, Washington D.C. และหลักสูตรการบริหารทรัพยากรเพื่อความมั่นคง (Defense Resource Management) ที่ Naval Postgraduate School, Monterey, CA ประเทศสหรัฐอเมริกา มีประสบการณ์การวิจัยหลายด้านเช่น Electromagnetic Interference and Compatibility (EMI/EMC), Mobile Cellular Communication, Satellite Communication, Broadband Communication และ ICT Management and Policy โดยมีผลงานตีพิมพ์ระดับนานาชาติทั้งในวารสารการประชุมระดับนานาชาติและวารสารวิจัยระดับนานาชาติที่เป็นที่ยอมรับมากกว่า 80 ฉบับ

การบริหารจัดการความมั่นคงระบบสารสนเทศ

“The Need for Security”

บทนำ

นโยบายและกลยุทธ์ด้านเทคโนโลยีสารสนเทศหลายๆ นโยบายและกลยุทธ์นั้นมีความแตกต่างกัน หน้าที่หลักของนโยบายและกลยุทธ์ป้องกันภัยข้อมูลสารสนเทศ เป็นสิ่งที่ทำให้แน่ใจว่าระบบสารสนเทศยังคงอยู่เหมือนเดิม โดยที่องค์กรนั้นจ่ายเงินเป็นหลักร้อยหลักพันดอลล่าร์สำหรับชั่วโมงการทำงานของพนักงานที่ทำหน้าที่ดูแลรักษาระบบสารสนเทศ ถ้าการคุกคามข้อมูลสารสนเทศและระบบยังไม่หมดไป องค์กรควรปรับปรุงระบบอย่างสม่ำเสมอ เพื่อสนับสนุนข้อมูลสารสนเทศ อย่างไรก็ตามการโจมตีระบบข้อมูลสารสนเทศเป็นเหตุการณ์ที่เกิดขึ้นเป็นประจำทุกวัน และต้องการการรักษาความปลอดภัยของข้อมูลสารสนเทศที่เพิ่มมากขึ้นพร้อมกับการโจมตีที่มีความซับซ้อนมากขึ้น

องค์กรต้องเข้าใจในสิ่งแวดล้อมของการทำงานของระบบข้อมูลสารสนเทศ ดังนั้นนโยบายและกลยุทธ์ป้องกันภัยข้อมูลสารสนเทศจึงจะสามารถจัดการปัญหาต่างๆ ได้ จะเห็นได้ว่าในบทนี้จะพูดถึงเรื่องสภาพแวดล้อมและการระบุถึงภัยคุกคาม ซึ่งเป็นต้นเหตุที่เกิดขึ้นกับข้อมูลสารสนเทศในองค์กร

สิ่งที่องค์กรต้องการ (Organization Need First)

การรักษาความปลอดภัยของข้อมูลสารสนเทศ มีส่วนประกอบสำคัญ 4 ส่วนได้แก่

1. การป้องกันการทำงานของระบบต่างๆในองค์กร
2. ปกป้องการดำเนินงานของโปรแกรมให้ปลอดภัย
3. การป้องกันข้อมูลที่องค์กรใช้และเก็บรวบรวม
4. ปกป้องทรัพย์สินเทคโนโลยีในองค์กร

การป้องกันการทำงานของระบบต่าง ๆในองค์กร (Protecting the Functionality or an Organization)

การจัดการทั่วไป และการจัดการทางด้าน IT ต่างมีภาระหน้าที่ที่จะต้องปกป้องการทำงานของระบบต่างๆในองค์กร ยังมีหน่วยงานธุรกิจ และหน่วยงานของรัฐจำนวนมาก หลบเลี่ยงที่จะจัดการปัญหาเรื่องความปลอดภัยของข้อมูล เพราะเห็นว่ามันเป็นงานที่มีเทคนิคซับซ้อน ซึ่งในความเป็นจริงการรักษาความปลอดภัยข้อมูลเน้นที่ **การจัดการ** มากกว่า **เทคโนโลยี** ขณะที่การทำบัญชีเงินเดือนก็เน้นเรื่องการจัดการมากกว่า การคำนวณด้วยคอมพิวเตอร์ ฉะนั้นการจัดการเรื่องการรักษาความปลอดภัยของข้อมูลนั้นขึ้นอยู่กับการกำหนดนโยบายและการบังคับใช้มาตรการต่างๆ ให้เกิดผลดังที่กำหนดไว้ มีข้อความเกี่ยวกับการรักษาความปลอดภัยข้อมูล เขียนโดย Charles Cresson Wood กล่าวว่า

“ในความเป็นจริงความปลอดภัยของข้อมูล เกิดจากการจัดการทางเทคโนโลยีสารสนเทศที่ดี ผู้คนจำนวนมากคิดที่จะแก้ไขเทคโนโลยีมากกว่าการแก้ปัญหาของเทคโนโลยี คิดเพียงว่าเป็นการดีไม่

ต้องมาเพิ่มงานฉันให้มากขึ้น เป็นเรื่องยากที่จะให้ผู้ใช้ใส่ใจกับมาตรการด้านการจัดการความปลอดภัยของข้อมูล ที่เพิ่มมาตรการด้านเทคนิคต่างๆ ด้วย”

การจัดการเรื่องความปลอดภัยข้อมูล ขึ้นอยู่กับการสื่อสารภายในองค์กรให้พนักงานเกิดความสนใจ ตระหนักในการรักษาความปลอดภัยข้อมูลของธุรกิจ ซึ่งมีผลกระทบกับค่าใช้จ่ายหากธุรกิจต้องหยุดชะงัก อย่างไรก็ต้องเน้นเรื่องความปลอดภัย เช่น การแก้ปัญหาทางเทคนิค

ปกป้องการดำเนินงานของโปรแกรมให้ปลอดภัย (Enabling the Safe Operation of Applications)

ทุกวันนี้องค์กรได้รับแรงกดดันอย่างมาก ที่จะต้องทำให้โปรแกรมต่างๆทำงานร่วมกันอย่างมีประสิทธิภาพ องค์กรสมัยใหม่จึงต้องการใช้โปรแกรมที่สามารถปกป้องระบบสารสนเทศขององค์กร โดยเฉพาะอย่างยิ่งโปรแกรมที่มีส่วนประกอบที่สำคัญต่อโครงสร้างพื้นฐานขององค์กร เช่น ระบบปฏิบัติการ จดหมายอิเล็กทรอนิกส์ และโปรแกรมสนทนา (IM) องค์กรอาจจะสร้างโปรแกรมด้วยการจ้างที่ปรึกษาจากภายนอก หรือ พัฒนาเอง ซึ่งโครงสร้างพื้นฐานขององค์กรแต่ละแห่งแผนกเทคโนโลยีสารสนเทศจะต้องจัดการตรวจสอบความปลอดภัยของระบบโครงสร้างพื้นฐานอย่างต่อเนื่อง ไม่ให้การทำงานของระบบต้องหยุดชะงัก

การป้องกันข้อมูลที่องค์กรใช้และเก็บรวบรวม (Protecting Data that Organizations Collect and Use)

หากองค์กรไม่มีการบันทึกข้อมูลการทำธุรกรรม ที่ต้องส่งยอดให้ลูกค้า ทุกธุรกิจไม่ว่าจะเป็นสถาบันการศึกษา หน่วยงานราชการ ที่มีการทำธุรกรรมซึ่งต้องอาศัยความน่าเชื่อถือในการให้บริการจากระบบสารสนเทศ แม้ว่าธุรกรรมที่ระบบข้อมูลไม่ได้ออนไลน์ การสร้างข้อมูล และการเคลื่อนไหวของสินค้าและบริการยังคงดำเนินการอยู่ เพราะฉะนั้นจะต้องให้ความสำคัญกับการปกป้องข้อมูลที่มีการเคลื่อนไหว และข้อมูลที่เหลือให้ได้รับความปลอดภัย ไม่ให้ข้อมูลถูกแฮกเกอร์ขโมย หรือ ทำการแก้ไขข้อมูล ระบบรักษาความปลอดภัยที่มีประสิทธิภาพต้องมีการวางแผนการป้องกัน เพื่อให้ข้อมูลขององค์กรมีความถูกต้องครบถ้วน ไม่ถูกแก้ไข

ปกป้องทรัพย์สินเทคโนโลยีในองค์กร (Safeguarding Technology Assets in Organization)

แม้องค์กรจะมีการปฏิบัติงานที่มีประสิทธิภาพ ยังคงต้องการเพิ่มบริการโครงสร้างพื้นฐานที่มีความปลอดภัยตามขนาดและขอบเขตขององค์กร เช่น ธุรกิจขนาดเล็กอาจจะมีผู้ให้บริการอินเตอร์เน็ตเป็นผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ และเครื่องมือในการสร้างรหัสส่วนบุคคล เมื่อองค์กรเติบโตจะต้องพัฒนาการบริการความปลอดภัยเพิ่มขึ้นด้วยเช่นกัน ยกตัวอย่าง การที่องค์กรขยายตัวเพิ่มขึ้นมีการทำธุรกรรมอิเล็กทรอนิกส์ ต้องทำให้ระบบได้รับความเชื่อถือ และมีความปลอดภัยในการติดต่อกับบุคคลและองค์กรภายนอก จะต้องมีเทคโนโลยีความปลอดภัยมาช่วยก็คือ Public Key

Infrastructure (PKI) เป็นการรวมกันของซอฟต์แวร์ระบบต่างๆ เช่น การสร้างรหัสลับ และ ข้อตกลงทางกฎหมายเพื่อสนับสนุนโครงสร้างพื้นฐานข้อมูลทั้งหมดขององค์กร รวมถึงใบรับรองอิเล็กทรอนิกส์ ลายมือชื่ออิเล็กทรอนิกส์ทำให้แน่ใจว่าการติดต่อธุรกิจผ่านทางอินเตอร์เน็ตเป็นความลับ ใบรับรองอิเล็กทรอนิกส์เป็นชุดข้อมูลอิเล็กทรอนิกส์มีข้อความและตัวเลขแสดงและระบุการมีตัวตนของผู้ถือใบรับรอง ทำให้แน่ใจว่าระบบสารสนเทศของผู้ให้บริการมีใบรับรอบอิเล็กทรอนิกส์ ข้อมูลต่างๆมีการตรวจสอบความถูกต้อง และผู้ใช้บริการจะได้ข้อมูลที่ถูกต้อง ครบถ้วน

ถ้าเครือข่ายขององค์กรมีการขยายตัว ควรจะมีการเปลี่ยนแปลงให้เหมาะกับความต้องการมากกว่าการแก้ไขเทคโนโลยี บางทีองค์กรมีความต้องการที่มากกว่าโปรแกรมรักษาความปลอดภัยที่มีอยู่ ตัวอย่างหนึ่งของการแก้ปัญหาเรื่องความแข็งแกร่งทางเทคโนโลยี คือ ไฟร์วอล เป็นอุปกรณ์ป้องกันเครือข่ายภายนอกออกจากเครือข่ายของเรา ให้เครือข่ายของเราได้รับความปลอดภัย

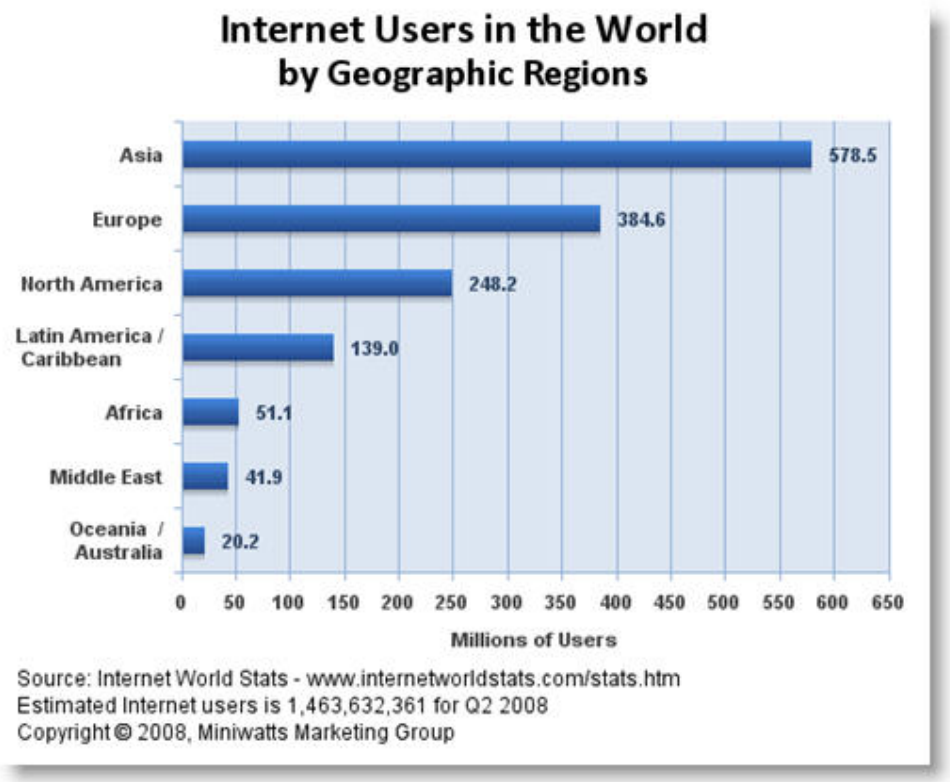
Threats

ประมาณ 500 ปี ก่อนคริตศักราช ชาวจีนชื่อ ซัน ซุน วู ได้เขียนเรื่อง Art of war ให้ความสำคัญกับการรู้จักตัวเองรวมถึงภัยคุกคามที่ต้องเผชิญ เพื่อจะได้รู้ว่าควรปกป้องข้อมูลขององค์กรอย่างไร สิ่งที่ควรรู้ คือ

1) รู้จักตัวเอง คือ รู้จักการปกป้องข้อมูลและระบบให้มีความมั่นคง ระบบขนส่ง และขั้นตอนต่างๆ

2) การรู้ถึงภัยคุกคามที่ต้องเผชิญ ศึกษาจากแหล่งข้อมูลที่น่าเชื่อถือทำให้สามารถตัดสินใจจัดการกับภัยคุกคามต่างๆที่มีผลกับ พนักงาน โปรแกรม ข้อมูล และระบบสารสนเทศขององค์กร การรักษาความปลอดภัยข้อมูล กล่าวถึงอันตรายจากภัยคุกคามที่ส่งผลกับคน และทรัพย์สิน

มีการสำรวจประเภทของภัยคุกคาม เมื่อการเชื่อมต่ออินเตอร์เน็ตขยายไปทั่วโลก ศึกษาถึงแนวทางปฏิบัติในการป้องกันภัยคุกคามต่างๆ มีการสำรวจเปรียบเทียบประเภทของภัยคุกคามทำให้เกิดความเข้าใจร่วมกันว่าภัยคุกคามที่เพิ่มขึ้นมาจากการที่องค์กรเชื่อมต่ออินเตอร์เน็ต โดยจำนวนผู้ใช้อินเตอร์เน็ตเพิ่มขึ้นเรื่อยๆ คิดเป็น 17% ของคนทั้งโลก หรือ จากคนทั่วโลก 6.6 พันล้านคน มีคนที่เข้าใช้งานอินเตอร์เน็ตถึง 1.1 พันล้านคน



รูปแสดงการใช้อินเตอร์เน็ตทั่วโลก

ปี 2006 Computer Security Institute (CSI) ซึ่งเป็นหน่วยงานของ FBI ทำการสำรวจอาชญากรรมคอมพิวเตอร์และการรักษาความปลอดภัย จากการศึกษาพบว่า 72% ที่ตอบสนอง (บริษัทขนาดใหญ่และหน่วยงานราชการ) ตรวจพบการฝ่าฝืนการรักษาความปลอดภัยทางอินเตอร์เน็ตภายใน 12 เดือนล่าสุด อีก 52% เข้าใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งลดลงจาก 56% ในปี 2005

ตารางต่อไป แสดง 12 ประเภทภัยคุกคามที่สร้างความเสียหายต่อพนักงาน ข้อมูลและระบบขององค์กร ทั้งนี้แต่ละองค์กรจะต้องจัดลำดับภัยคุกคามที่ต้องเผชิญ โดยเฉพาะกำหนดกลยุทธ์ความปลอดภัยในการกำจัดความเสี่ยง และแสดงระดับการจัดการทรัพย์สิน ในบทที่ 4 จะครอบคลุมหัวข้อต่างๆได้ละเอียดมากกว่า

คุณสามารถดูตัวอย่างภัยคุกคามได้จากตาราง แสดงรายการมากกว่าหนึ่งประเภท

ตาราง **Threats to Information Security**

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

1. ข้อผิดพลาดจากการกระทำของมนุษย์ (Acts of human error or failure)

ประเภทนี้มีการกระทำโดยเจตนา หรือ มีเจตนามุ่งร้ายโดยผู้ใช้ที่มีสิทธิ์เข้าใช้ระบบ เมื่อผู้ใช้ระบบทำงานผิดพลาด เนื่องจากขาดความชำนาญ ขาดการฝึกอบรม และการสันนิษฐานไม่ถูกต้อง สิ่งเล็กน้อยเหล่านี้สามารถสร้างความเสียหายอย่างมาก

การคุกคามที่อันตรายที่สุดต่อความปลอดภัยของข้อมูลองค์กร คือ พนักงานขององค์กรเอง เพราะพนักงานใช้ข้อมูลในการดำเนินกิจกรรมทางธุรกิจขององค์กรทุกวัน สิ่งที่พนักงานจะต้องปฏิบัติอย่างเคร่งครัดคือ การรักษาความลับของข้อมูล ข้อมูลมีความถูกต้องครบถ้วน และข้อมูลพร้อมใช้งานได้ทุกเมื่อ รูปต่อไปเป็นการแนะนำเกี่ยวกับการคุกคามจากภายนอก เพราะความผิดพลาดเพียงเล็กน้อยของพนักงาน เช่น ไม่ได้ปิดประตูหน้าต่างทำให้หัวขโมยเข้ามาในองค์กรได้ การลบหรือแก้ไขข้อมูลที่เป็นเอกสารสำคัญ

รูปแสดงข้อผิดพลาดของมนุษย์

2. การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property)

ทรัพย์สินทางปัญญา (IP) เป็นส่วนหนึ่งของการดำเนินธุรกิจ ซึ่งทรัพย์สินทางปัญญา เป็นผลงานของผู้ที่เป็นเจ้าของความคิด และเป็นทรัพย์อีกชนิดหนึ่ง ได้แก่ ลิขสิทธิ์ เครื่องหมายการค้า และสิทธิบัตร คุณสมบัติของทรัพย์สินทางปัญญาอย่างหนึ่งคือ มีการระบุรหัสบ่งชี้ไว้อย่างเหมาะสม

บ่อยครั้งที่องค์ซื้อหรือทำสัญญาเช่าทรัพย์สินทางปัญญาจากองค์กรอื่น ต้องปฏิบัติตามข้อตกลงที่ได้ทำไว้เพื่อความยุติธรรมและความรับผิดชอบในการนำไปใช้ ส่วนใหญ่การละเมิดทรัพย์สินทางปัญญาจะเป็นการทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์ ซึ่งเป็นการกระทำที่ผิดกฎหมาย

ผู้ผลิตซอฟต์แวร์ใช้เทคนิควิธีในการควบคุม เพื่อป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ นอกเหนือจากกฎหมายต่อต้านการละเมิดลิขสิทธิ์ซอฟต์แวร์ ยังมี 2 องค์กร ที่คอยเฝ้าระวังการละเมิดลิขสิทธิ์ คือ SIIA, BSA เมื่อเร็วๆ BSA สำรวจเมื่อเดือนพฤษภาคม 2006 เปิดเผยว่าเศษหนึ่งส่วนสามของซอฟต์แวร์ที่ใช้ในโลกเป็นซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ องค์กรเหล่านี้แสดงรายละเอียด และวิธีปฏิบัติ เพื่อป้องกันการละเมิดสิทธิ์ในทรัพย์สินทางปัญญา และมีเทคนิควิธีจำนวนมากที่ใช้ตรวจสอบ เช่น ลายน้ำดิจิตอล การฝังรหัสลิขสิทธิ์ เป็นเจตนาทำให้เกิด bad sectors บนสื่อที่บรรจุซอฟต์แวร์ เพื่อให้มีการปฏิบัติตามกฎหมายลิขสิทธิ์

3. การบุกรุก (Deliberate Acts of Trespass)

การบุกรุกจากภายนอกเป็นสิ่งที่ได้รับการกล่าวถึงอย่างมาก ทั้งในรูปแบบที่เป็นอิเล็คทรอนิกส์ และกระทำโดยคนที่สามารถเข้าถึงข้อมูลที่เป็นความลับ เมื่อมีบุคคลที่ไม่ได้รับอนุญาตได้ทำการรุกล้ำและพยายามเข้าถึงข้อมูลขององค์กรที่มีการป้องกัน ซึ่งพฤติกรรมดังกล่าวเป็นการบุกรุกโดยยเจตนา

นักโจมตีระบบสามารถที่จะใช้วิธีการต่าง ๆ ในการเข้าถึงข้อมูลที่เก็บรักษาอยู่ภายในระบบสารสนเทศ ตัวอย่างเช่น ข้อมูลที่มีการจัดเก็บและรวบรวมโดยการใช้ Web Browser ในการทำวิจัยทางการตลาด วิธีการดังกล่าวเรียกว่า การหาข้อมูลของคู่แข่ง (Competitive Intelligence) ซึ่งถือว่าเป็นการจารกรรมข้อมูลทางอุตสาหกรรม (Industrial Espionage) เป็นการกระทำที่ผิดกฎหมาย

กลุ่มประเทศที่เป็นพันธมิตรกับทางอเมริกา จึงได้มีการจัดตั้งองค์กรต่อต้านการจารกรรมข้อมูลทางอุตสาหกรรม จะเห็นได้ว่าในนานาประเทศได้ให้ความสำคัญต่อการป้องกันภัยคุกคามและการจารกรรมข้อมูล โดยการมีส่วนร่วมอย่างจริงจังในการรักษาความปลอดภัยในระดับสากล

รูปแบบของการจารกรรมข้อมูล

Shoulder Surfing การยืนข้างหลังมองข้ามไหล่ เป็นรูปแบบการจารกรรมข้อมูลแบบธรรมดาที่ไม่มีการใช้เทคโนโลยีใด ๆ มาช่วย คือ การแอบดูหรือจำข้อมูลที่เป็นความลับของผู้อื่น เช่น การแอบดูรหัสผ่านของบัตร ATM ขณะที่ทำการทำรายการ, รหัสในการเข้าใช้งานระบบคอมพิวเตอร์ของบุคคลอื่น, รหัสผ่านของเครื่องโทรศัพท์ขณะที่มีการทำรายการผ่านทางโทรศัพท์ เป็นต้น

โดยปกติไม่ได้มีการเขียนเป็นข้อบังคับหรือข้อห้ามโดยชัดเจนในการแอบดูข้อมูลความเป็นส่วนตัวของผู้อื่น เนื่องจากถือเป็นมรรยาทที่ทุกคนควรปฏิบัติโดยปกติอยู่แล้ว ดังนั้นเจ้าของข้อมูลที่เป็นส่วนตัวจะต้องป้องกันตนเองเป็นอันดับแรกจากภัยคุกคามในรูปแบบนี้

Hacker นักเจาะระบบที่มีความเชี่ยวชาญในการเขียนโปรแกรมที่สามารถจะเข้าถึงข้อมูลที่มีการป้องกันอย่างผิดกฎหมาย ซึ่งโดยส่วนใหญ่จะเป็นการกระทำเพื่อทดสอบความสามารถของตนเอง ชอบสิ่งที่ท้าทายหรือลี้ลับที่ต้องการค้นหา โดยการทุ่มเทเวลาในการเขียนโปรแกรม โดยใช้ความรู้ที่มีอยู่และค้นคว้าเพิ่มเติม ในการที่พยายามจะเจาะระบบที่มีการรักษาความปลอดภัยที่แน่นหนา เป็นเป้าหมายหลัก

วิวัฒนาการของ Hacker (Hacker profiles)

ในยุคแรก ๆ Hacker ส่วนมากจะเป็นเพศชาย มีอายุระหว่าง 13-18 ปี ซึ่งขาดการดูแลเอาใจใส่จากผู้ปกครอง และใช้เวลาส่วนใหญ่อยู่กับการใช้เครื่องคอมพิวเตอร์

ในปัจจุบัน Hacker จะไม่มีการจำกัดเพศ และมีช่วงอายุที่เปลี่ยนไปคือ ระหว่าง 12-60 ปี ประวัติหรือภูมิหลังไม่เป็นที่รู้จัก เนื่องจากความเปลี่ยนแปลงทางเทคโนโลยี ระดับความรู้ต่าง ๆ และ Hacker อาจจะเป็นบุคคลจากภายในหรือภายนอกองค์กรก็ได้

ประเภทของ Hacker ตามระดับความสามารถ แบ่งได้ออกเป็น 2 กลุ่ม คือ

1. Expert Hacker หรือ Elite Hacker
2. Novice Hacker หรือ Unskilled Hacker

Expert Hacker ส่วนใหญ่จะเป็นผู้ที่มีทักษะขั้นสูงในการเขียนโปรแกรมได้หลากหลายภาษา รวมถึงความรู้เกี่ยวกับการทำงานของระบบเครือข่ายและระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ และมีคุณลักษณะพิเศษคือ มีความกระตือรือร้นและทุ่มเทเวลา ในการพยายามที่จะเจาะระบบความ

ปลอดภัยขั้นสูงของผู้อื่น ดังนั้นเมื่อกลุ่มเป้าหมายที่ถูกเลือกแล้วมีโอกาสหรือความเป็นไปได้สูงที่ระบบความปลอดภัยจะถูกบุกรุกหรือคุกคามโดย Expert Hacker ในการโจมตีหรือเจาะระบบจะมีการประกาศหรือแจ้งให้รู้โดยตรงด้วยการเขียนไว้ในโปรแกรมที่ใช้ในการบุกรุกระบบ

Novice Hacker เป็น Hacker ที่มีความรู้หรือทักษะในการเขียนโปรแกรมจำกัดและไม่สามารถที่จะพัฒนาโปรแกรมที่เจาะระบบได้เหมือนกับ Expert Hacker จะเป็นการใช้โปรแกรม Hack สำเร็จรูปที่เขียนขึ้นโดย Expert Hacker มาเป็นเครื่องมือในการโจมตีระบบรักษาความปลอดภัยอีกทีหนึ่ง เรียกว่า Script Kiddies หรือ Packet Monkey โดยที่ Novice Hacker จะไม่สามารถทราบถึงกลไกหรือกระบวนการทำงานภายในโปรแกรม Script Kiddies จะเป็นลักษณะการโจมตีที่ก่อกวนเครือข่ายคอมพิวเตอร์เป็นส่วนใหญ่ (Denial-of-service) Novice Hacker สามารถหาโปรแกรมที่เป็น Script Kiddies โดยการ Download จาก Internet ซึ่ง Expert Hacker นำไปเผยแพร่ไว้ ในทางกลับกันผู้ดูแลรักษาความปลอดภัยของระบบก็สามารถที่จะค้นพบโปรแกรมเหล่านี้ได้เช่นกัน ทำให้เกิดนักพัฒนาโปรแกรมหรืออุปกรณ์ที่นำมาใช้ป้องกันระบบจากการโจมตีหรือการบุกรุกจากภายนอก

ในเดือนกุมภาพันธ์ ปี 2000 มี Hacker หนุ่ม ที่ใช้ชื่อว่า Mafiaboy ถูกจับเนื่องจากเข้าไปโจมตีและก่อกวนระบบเครือข่ายของ Web site โดยถูกตัดสินให้จำคุก 8 เดือน และ ถูกปรับเป็นเงิน 250 ดอลล่าร์ บริจาคให้การกุศล สาเหตุที่ทำให้ต้องถูกจับเนื่องจากไม่สามารถที่จะลบ System Logs ที่ตรวจจับการกระทำการบุกรุกของ Mafiaboy และจากการที่ได้ไปแสดงตัวหรือโอ้อวดถึงการกระทำดังกล่าวในห้องสนทนาทางอินเตอร์เน็ต

Cracker จะเป็นการถอดรหัสหรือทำลายโปรแกรมที่ใช้ในการป้องกันการทำข้อมูลซ้ำ ซึ่งเป็นนการกระทำที่ละเมิดลิขสิทธิ์ โปรแกรมประเภท Cracker สามารถที่จะเผยแพร่และติดตั้งได้อย่างง่ายดาย

ความหมายของ Hacker และ Cracker จะพิจารณาจากเจตนาของกระทำความผิดเป็นหลัก Hacker ไม่ได้มุ่งเน้นในการทำลายข้อมูลหรือสร้างความเสียหาย ส่วน Cracker จะมุ่งเน้นในการทำลายข้อมูลหรือสร้างความเสียหายต่าง ๆ ให้เกิดขึ้นกับระบบ

Phreaker เป็นการโจมตีเครือข่ายโทรศัพท์สาธารณะทำให้สามารถใช้งานได้โดยไม่เสียค่าใช้จ่ายหรือทำให้การบริการเกิดความยุ่งเหยิงขึ้น Phreaker มีชื่อเสียงโด่งดังในปี 1970 เมื่อมีการพัฒนาอุปกรณ์ชนิดหนึ่งเรียกว่า Blue Boxes ที่สามารถใช้งานโทรศัพท์ที่ต้องจ่ายค่าบริการ โดยไม่ต้องจ่ายค่าบริการแต่อย่างใด หลังจากนั้นมีการพัฒนา Red Boxes เป็นอุปกรณ์ใช้สร้างเสียงจำลองการหยอดเหรียญในเครื่องโทรศัพท์ที่ต้องจ่ายค่าบริการ

4. การกรรโชกข้อมูลสารสนเทศ (Deliberate Acts of Information Extortion)

การขู่กรรโชกในการเปิดเผยข้อมูลที่เป็นความลับเกิดขึ้นจากการที่ข้อมูลที่เป็นความลับที่จัดเก็บอยู่ในระบบถูกขโมยไปอาจจะเป็นผู้บุกรุกจากภายนอกหรือผู้ที่มีหน้าที่ดูแลรักษาข้อมูลภายในองค์กร โดยมีการเรียกร้องค่าตอบแทนหรือค่าไถ่(Ransom) แลกกับการที่จะไม่เปิดเผยข้อมูลความลับที่ได้ขโมยมา (Black Mail) ส่วนมากจะเป็นการขู่กรรโชกข้อมูลหมายเลขบัตรเครดิตที่ได้ขโมยมา

ตัวอย่างของ Web-Base CD Universe ที่ตกเป็นเหยื่อของการขโมยแฟ้มข้อมูลที่จัดเก็บข้อมูลหมายเลขบัตรเครดิตของลูกค้า โดยผู้ที่ทำการขโมยข้อมูลเป็น Hacker ชาวรัสเซีย ชื่อ Maxus ซึ่งได้ขโมยข้อมูลบัตรเครดิตไปเป็นจำนวนหลายแสนใบ โดยบริษัท CD Universe ปฏิเสธการจ่ายเงินตามคำขู่ที่จะเปิดเผยข้อมูลความลับนี้ มูลค่า 100,000 ดอลล่าร์ นาย Maxus ได้ทำการ Post หมายเลขบัตรเครดิต ไปใน Web Site เพื่อเสนอขายข้อมูลให้กับกลุ่มคนที่ก่ออาชญากรรม ส่งผลให้ Web Site ได้รับความนิยมเป็นอย่างมากจนจะต้องจำกัดสิทธิ์ของผู้ที่จะเข้ามาดูข้อมูลที่เสนอขาย

ตัวอย่าง เหตุการณ์ขู่กรรโชกที่เกิดขึ้นในเดือนมิถุนายน ปี 2000 เมื่อมีนักเรียนถูกกล่าวหาว่ากระทำการข่มขู่ว่าจะเปิดโปงความลับ (Online Blackmail) โดยจะทำการเปิดเผยวิธีการ Download หนังสือจากบริษัท Digital Book โดยไม่ต้องเสียค่าใช้จ่าย ยกเว้นเสียจากจะมีการจ่ายเงินให้ก้อนโต โดยในปี 2001 ได้ไปก่อคดีเดียวกันเพิ่มเติมอีก ซึ่งโทษของการข่มขู่ที่จะเปิดโปงความลับ (Blackmail) คือ จำคุก 2 ปี และปรับเพิ่ม 100,000 ดอลล่าร์ แต่ในกรณีของนักเรียนรายนี้โทษสูงสุดคือ จำคุก 36 ปี และ ปรับเพิ่ม 800,000 ดอลล่าร์

5. การก่อวินาศกรรมหรือการทำลาย (Deliberate Acts of Sabotage or Vandalism)

การมีส่วนร่วมในการป้องกันภัยคุกคามการก่อวินาศกรรมระบบคอมพิวเตอร์หรือธุรกิจ หรือการกลั่นแกล้งทำลายทรัพย์สินก่อให้เกิดความเสียหาย เช่น การทำลายทรัพย์สิน หรือ การทำลายภาพพจน์ที่ดีขององค์กร

การกลั่นแกล้งทำลายทรัพย์สินเล็ก ๆ น้อย ๆ โดยพนักงาน สามารถนำไปสู่เหตุการณ์การก่อวินาศกรรมต่อองค์กร ในบางครั้งการสร้างความเสียหายไม่จำเป็นต้องเป็นตัวเงินเสมอไป การโจมตีภาพพจน์ขององค์กรก็เป็นเรื่องร้ายแรงเช่นเดียวกัน การทำลาย Web Site ส่งผลกระทบต่อความเชื่อมั่นของลูกค้าทำให้ยอดขายและมูลค่าขององค์กร รวมถึงชื่อเสียงก็ลดลงเช่นกัน

ตัวอย่างเมื่อ วันที่ 13 กรกฎาคม ปี 2001 กลุ่ม Fluffi Bunni ได้ขึ้นข้อความที่หน้า Web Site ของ SANS ว่า

“ท่านยังสามารถให้ความไว้วางใจคนเหล่านี้ สอนเรื่องการรักษาความปลอดภัยกับท่านได้จริงหรือ”

เหตุการณ์ที่เกิดขึ้นนี้ทำให้ SANS ต้องเสื่อมเสียชื่อเสียง นับตั้งแต่ได้มีการก่อตั้งสถาบันในการจัดการให้ความรู้และออกเอกสารรับรองทางด้านระบบความปลอดภัย

สถาบัน SANS มาจากคำว่า SysAdmin, Audit, Network, Security ซึ่งก่อตั้งขึ้นจากความร่วมมือในศึกษาค้นคว้าและฝึกฝนและรวบรวมเกี่ยวกับการรักษาความปลอดภัย

มีรายงานจำนวนนับไม่ถ้วนของนักเจาะระบบ (Hacker) ที่สามารถเข้าไปในระบบและทำความเสียหายหรือทำลายข้อมูลที่จำเป็น ในกรณีของ Web Site รายงานเกี่ยวกับการเจาะระบบและแลกเปลี่ยนข่าวกรอง ได้ถูกเจาะเข้าในระบบ ผลกระทบที่เกิดขึ้นคือจำนวนรายงานการเจาะระบบเพิ่มขึ้นอย่างมหาศาล จนทำให้ Attrition.com ต้องระงับการแจ้งบัญชีรายชื่อใน Web Site ทั้งหมด โดยเปลี่ยนเป็นวิธีรับอาสาสมัครมาทำการปรับปรุงข้อมูลบน Web แทนการแจ้งผ่านหน้า Web Site

ผู้เชี่ยวชาญด้านความปลอดภัย ได้ออกมาประกาศเตือนเกี่ยวกับการทำลายการเชื่อมต่อเครือข่าย Internet ในรูปแบบอื่น คือ ปฏิบัติการ Hactivist หรือ Cyberactivist ซึ่งจะเป็นการแทรกแซงหรือทำให้ระบบเกิดความสับสน โดยปฏิเสธในการปฏิบัติตามนโยบายและการกระทำที่กำหนดโดยองค์กร หรือ หน่วยงานรัฐบาล

ความน่ากลัวอย่างที่สุดคือ ลักธิก่อการร้ายทางอินเตอร์เน็ต (Cyberterrorism) ผู้ก่อการร้ายทางอินเตอร์เน็ตจะทำการเจาะเข้าในระบบจากนั้นจะปฏิบัติการก่อการร้ายโดยผ่านทางเครือข่ายหรือใช้เส้นทางของอินเตอร์เน็ต สหรัฐอเมริการและรัฐบาลของนานาประเทศกำลังร่วมกันพัฒนาเครื่องมือรักษาความปลอดภัย โดยมุ่งมั่นที่จะป้องกันคอมพิวเตอร์ที่จำเป็น เครือข่ายการติดต่อสื่อสาร และโครงสร้างพื้นฐานทางกายภาพและด้านพลังงาน

ลัทธิก่อการร้ายทางอินเตอร์เน็ต ได้ปรากฏออกมาในช่วงระหว่างสงครามในโคโซโว บนหน้า Web site ของ NATO เป็นความพยายามของผู้สังเกตการณ์บางส่วน นำเอาสถานะของลักธิก่อการร้ายทางอินเตอร์เน็ตที่ไม่ได้ทำการคุกคามจริง เพื่อหันเหความสนใจจากการออกประกาศบังคับใช้การรักษาความปลอดภัยสารสนเทศให้เป็นรูปธรรม

จากบันทึกของ Dr. Mudawi Mukhtar Elmusharaf ศูนย์วิจัยด้านการก่ออาชญากรรมทางคอมพิวเตอร์ (Computer Crime Reserch Center เมื่อวันที่ 21 ตุลาคม 2002 เกี่ยวกับการพุ่งโจมตีของ DDOS (Distributed Denial-of-service) ไปยัง 13 เซิร์ฟเวอร์หลัก ที่ทำหน้าที่จัดเส้นทางของการติดต่อของอินเตอร์เน็ตทั้งหมด โดยจำนวน 9 ใน 13 เซิร์ฟเวอร์ การจราจรของเครือข่ายเต็มหมดทำให้การทำงานของเครื่องช้าลง ปัญหาที่เกิดขึ้นได้รับการแก้ไขในระยะเวลาอันสั้น แต่สถิติการโจมตีและผลที่เกิดขึ้นไม่ได้มีการประกาศออกไปให้ผู้ใช้อินเตอร์เน็ตส่วนใหญ่ได้ทราบข่าวดังกล่าว

6. การโจรกรรม (Deliberate Acts of Theft)

การคุกคามโดยการโจรกรรม จากบุคคลที่ได้มีการไตร่ตรองไว้ล่วงหน้า โดยมีเจตนายึดทรัพย์สินของผู้อื่นไปครอบครองโดยผิดกฎหมาย ซึ่งภายในองค์กรสามารถถูกโจรกรรมทรัพย์สินดังต่อไปนี้

ทรัพย์สินทางกายภาพ (Physical Property) เช่น เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เป็นต้น

แนวทางการป้องกัน

- การตรวจนับจำนวนทรัพย์สินสม่ำเสมอ
- ทำการล็อคประตูและมีการจัดอบรมเจ้าหน้าที่ด้านความปลอดภัย
- ติดตั้งระบบสัญญาณเตือนภัย

ทรัพย์สินทางอิเล็กทรอนิกส์ (Electronic Property) มีความซับซ้อนในการจัดการและควบคุม ซึ่งเป็นปัญหาขององค์กร ซึ่งต่างจากการโจรกรรมทรัพย์สินทางกายภาพสามารถตรวจพบได้ง่ายกว่า เมื่อทรัพย์สินทางอิเล็กทรอนิกส์ถูกขโมยไป องค์กรส่วนใหญ่จะทราบว่าทรัพย์สินถูกโจรกรรมมักจะสายเกินไป เนื่องจากนักโจรกรรมได้ทำการปกปิดร่องรอยการกระทำความผิดอย่างระมัดระวัง

ทรัพย์สินทางปัญญา (Intellectual Property) มูลค่าของข้อมูลจะลดน้อยลง ถ้าถูกขโมยไปโดยปราศจากความรู้ของเจ้าของทรัพย์สิน

7. การโจมตีซอฟต์แวร์ (Deliberate Software Attacks)

การโจมตีซอฟต์แวร์ เกิดขึ้นโดยการออกแบบซอฟต์แวร์ให้โจมตีระบบจากคนๆ เดียวหรือจากกลุ่มคนมีซอฟต์แวร์ที่ก่อความเสียหาย ทำลาย หรือ ปฏิเสธการบริการของระบบเป้าหมาย ซอพต์แวร์ที่ได้รับความนิยมคือ Malicious Code หรือ Malicious Software มักจะเรียกว่า มัลแวร์ (Malware) มีมากมาย อาทิ ไวรัส (Viruses) เวิร์ม (Worms) ม้าโทรจัน (Trojan Horses) Logic bombs และ ประตูหลัง (Back doors)

เรื่องราวของการโจมตีซอฟท์แวร์ที่โด่งดังโดยเฉพาะผลกระทบของ Malicious Code โดยใช้วิธีโจมตีระบบจนทำให้เครื่องไม่สามารถให้บริการได้ตามปกติ (Denial-of-Service) โดย Mafiaboy บน Web site Amazon.com, CNN.com, Etrade.com, ebay.com, Yahoo.com, Excite.com, และ Dell.com โดยใช้เวลาในการโจมตีประมาณ 4 ชั่วโมง มีรายงานว่าความเสียหายทำให้สูญเสียรายได้ล้านดอลลาร์ ต่อไปจะเป็นการอธิบายถึงภัยคุกคามจากมัลแวร์ ประกอบด้วย

Virus

ไวรัสคอมพิวเตอร์ประกอบด้วยส่วนของโค๊ดทำหน้าที่มุ่งร้าย ซึ่งโค๊ดนี้จะทำตัวคล้ายกับเชื้อไวรัสที่โจมตีสัตว์ และพืช โดยสามารถแพร่กระจายได้ด้วยตัวเอง คอมพิวเตอร์ที่มีโปรแกรมไวรัสอยู่ไวรัสจะเข้าไปควบคุมการทำงานของคอมพิวเตอร์ให้ทำงานผิดปกติ และแพร่กระจายไวรัสเข้าไปในระบบ บ่อยครั้งผู้ใช้ทำให้ไวรัสเข้าสู่ระบบโดยรู้เท่าไม่ถึงการณ์ เช่น การเปิดอีเมล์ หรือการสุ่มส่งป๊อปอัพไป หากผู้ใช้ไม่ตรวจสอบไฟล์ที่ได้รับแล้วเปิดอ่านเลย ข้อมูลและฮาร์ดไดร์จะถูกทำลายทั้งหมด ไวรัสสามารถส่งผ่านจากเครื่องหนึ่งไปสู่อีกเครื่องได้ผ่านสื่อต่างๆ อีเมล์ หรือการส่งข้อมูลทางคอมพิวเตอร์ เมื่อเครื่องติดไวรัสแล้วมันจะแพร่กระจายไปกับอีเมล์ หรือการส่งไปยังผู้ใช้ทุกคนที่มีชื่ออยู่ในสมุดที่อยู่

วิธีที่ใช้มากที่สุดในการส่งไวรัสในศตวรรษที่21 คือการแนบไฟล์ไปกับอีเมล์ องค์กรจำนวนมากป้องกันอีเมล์ด้วยการเลือกอีเมล์ที่ไว้ใจได้ และการกรองอีเมล์ทั้งหมดซึ่งรู้ว่าอีเมล์ใดมีไวรัสบ้าง ไวรัสใช้เวลาเพียงเล็กน้อยในการติดตั้งโปรแกรมไวรัสด้วยแผ่นดิสก์แล้วกระจายไปยังระบบต่างๆ

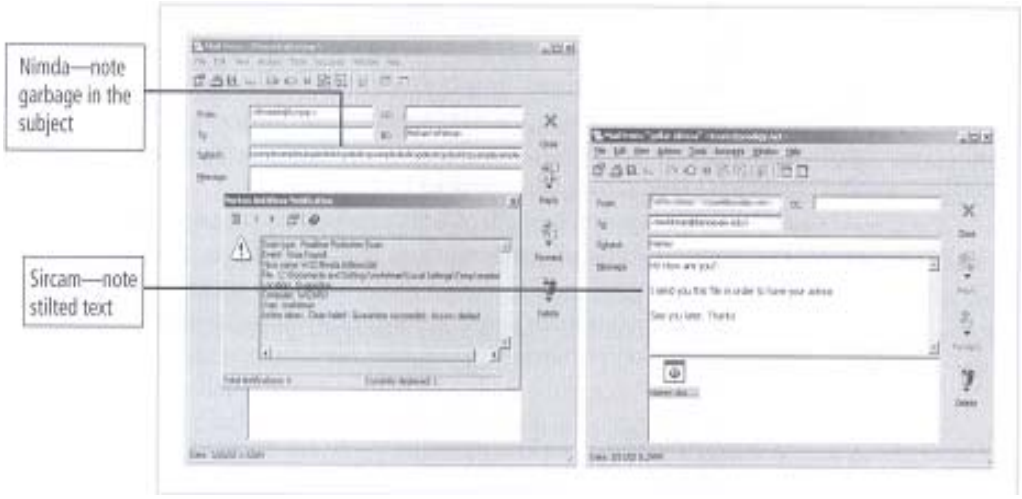
ปัจจุบันเครื่อข่ายคอมพิวเตอร์และโปรแกรมตรวจสอบอีเมล์ เพื่อจัดการไวรัสมีอยู่มาก ผู้จำหน่ายซอฟต์แวร์ป้องกันไวรัสที่ได้รับการยอมรับมีดังนี้ Symantec Norton Anti-Virus และ McAfee VirusScan มีโปรแกรมช่วยในการจัดการไวรัสคอมพิวเตอร์ได้

ในจำนวนชนิดของไวรัสคอมพิวเตอร์ในระบบเป็นไวรัสที่เขียนขึ้นมาเอง (macro virus) ด้วยการฝังชุดคำสั่งลงไปที่ระบบปฏิบัติการของเครื่องคอมพิวเตอร์โดยอัตโนมัติ เมื่อมีการใช้โปรแกรมเวิร์ด เอ็กเซลล์ และระบบฐานข้อมูล ไวรัสจะเริ่มทำงาน ซึ่งไฟล์ของระบบปฏิบัติการจะติดไวรัสที่ชุดคำสั่งในการเปิดเครื่อง (boot sector)

Worms

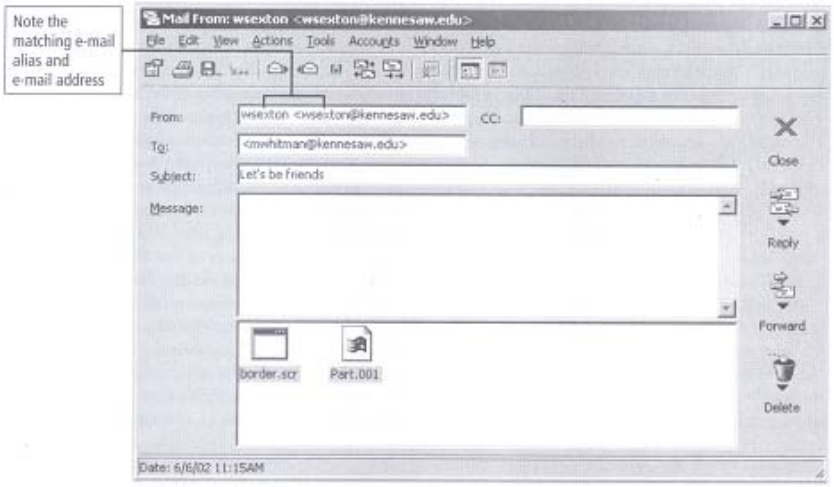
Worms เป็นโปรแกรมที่มุ่งร้ายต่อเครื่องคอมพิวเตอร์ สามารถจำลองตัวเองได้ตลอด ใช้ทรัพยากรของเครื่อง เช่น หน่วยความจำ พื้นที่ฮาร์ดดิสก์ และความเร็วของเครือข่าย เวิร์มทำงานได้แม้ไม่ได้ออนไลน์ Robert Morris และเวิร์มที่สามารถสร้างความเสียหายมากได้แก่ Code Red, Sircam, Nimda และ Klez

ตัวอย่างรูปแบบของเวิร์มที่เป็นการโจมตีในแบบ single package ตามรูป



รูปแสดง Nimda and Sircam Viruses

เวิร์มมีการเปลี่ยนแปลงรูปแบบการแพร่กระจายตัวเองจำนวนมากดังรูปข้างล่าง เป็นแบบ double-barreled payload ซึ่งเวิร์มจะส่งเมล์จำนวนมากและแนบตัวเองไปกับอีเมล์ด้วย เวิร์มที่มีการจู่โจมแบบแพร่กระจายนี้ได้แก่ MS-Blaster, MyDoom และ Netsky โดยเวิร์มและไวรัสมีการเปลี่ยนแปลงการโจมตีจุดอ่อนของระบบปฏิบัติการและแอพพลิเคชั่นได้หลายรูปแบบ

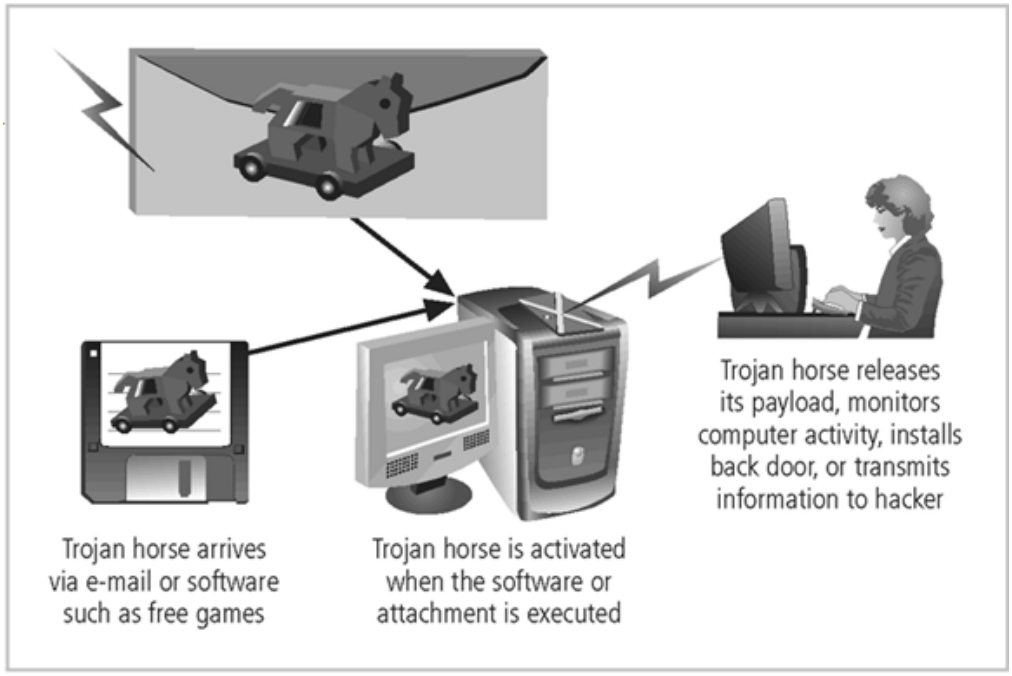


รูปแสดง Klez Virus

Trojan horses

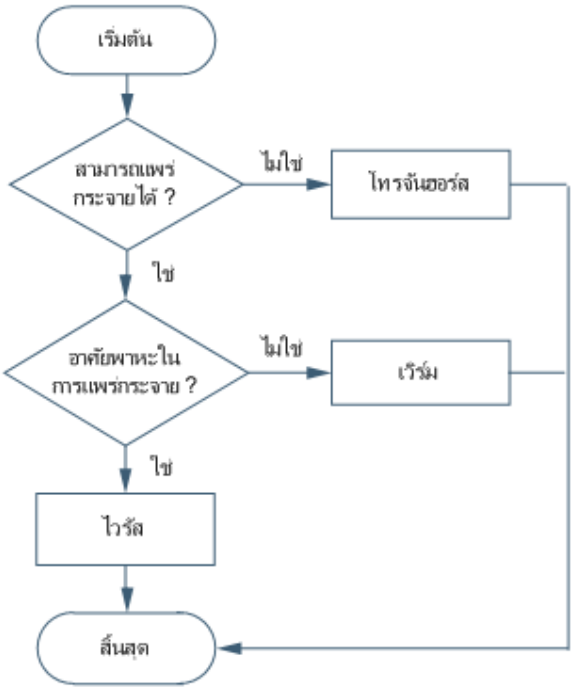
โทรจันฮอร์สจะแฝงตัวมากับซอฟต์แวร์ จะทำงานเมื่อผู้ใช้รันซอฟต์แวร์ แล้วโทรจันฮอร์สจะทำลายระบบคอมพิวเตอร์ เช่น เมื่อเรียกไฟล์ .exe ที่มากับแชร์แวร์ หรือ ฟรีแวร์

รูปแสดงตัวอย่างสรุปการโจมตีของโทรจันฮอร์ส ประมาณ 20 มกราคม 1999 เริ่มจากผู้ใช้ได้รับอีเมล์ที่มีโปรแกรมโทรจันฮอร์สแนบมาชื่อ Happy99.exe เมื่อเปิดอีเมล์และติดตั้งโปรแกรมโทรจันฮอร์สที่แฝงมาจะก่อกวนระบบทันที เช่น ลบไฟล์ หรือ สร้างแบ็คดอร์ให้แฮคเกอร์เข้ามาขโมยข้อมูล ลบไฟล์ต่างๆในระบบได้



รูปแสดง Trojan Horse Attack

แผนผังแสดงความแตกต่างของมัลแวร์



รูปสรุปแผนผังความแตกต่างของมัลแวร์

Back Door or Trap Door

Back door หรือ Trap door เป็นสิ่งที่โปรแกรมเมอร์ได้สร้างไว้และรู้กันเฉพาะกลุ่มสำหรับการเข้าไปแก้ไขระบบ ซึ่งเป็นช่องโหว่ให้แฮคเกอร์เข้ามาในระบบและมีสิทธิพิเศษในการแก้ไขสิ่งต่างๆ ตัวอย่าง ประเภทของ back door มี Subseven และ Back Orifice

Polymorphism

Polymorphism เป็นไวรัสชนิดหนึ่งที่ได้รับการพัฒนาให้มีความยากในการตรวจจับ อาจจะใช้เวลาหลายวันในการสร้างโปรแกรมตรวจจับ เพื่อจัดการกับ polymorphism เพราะมันใช้เทคนิคการซ่อนลักษณะเฉพาะที่สำคัญ (signatures) ไม่ให้คงรูปเดิม เพื่อหลีกจากการตรวจจับของโปรแกรมแอนตี้ไวรัส

Virus and Worm Hoaxes

เป็นรูปแบบของการหลอกลวงผู้ใช้คอมพิวเตอร์ทำให้เสียเงินเสียเวลาในการวิเคราะห์ โดยไวรัสหลอกลวงจะมาในรูปจดหมายอิเล็กทรอนิกส์ เตือนให้ระวังอันตรายจากไวรัส ด้วยการอ้างแหล่งข้อมูลเป็นรายงานที่น่าเชื่อถือ เพื่อให้ผู้รับส่งต่อจดหมายเตือนฉบับนั้นต่อๆไปอีกหลายๆทอด ซึ่งเป็นลักษณะของไวรัสหลอกลวง หากได้รับจดหมายประเภทนี้ไม่ควรที่จะส่งต่อ ควรเช็คจากแหล่งข้อมูลที่ถูกต้องก่อนทำการส่ง และควรจะอัพเดทโปรแกรมแอนตี้ไวรัสอย่างสม่ำเสมอ

แหล่งข้อมูลทางอินเตอร์เน็ทในการวิจัยเกี่ยวกับไวรัสว่าจริงหรือหลอก สำหรับข้อมูลล่าสุดของภัยคุกคามทั้งไวรัส เวิร์ม และโฮแอ็กส์ สามารถเข้าไปได้ที่ CERT Coordination (www.cert.org) เป็นศูนย์รวมการรักษาความปลอดภัยข้อมูล

8. ภัยธรรมชาติ (Forces of Nature)

ภัยธรรมชาติเป็นภัยคุกคามที่อันตรายมาก เพราะเป็นสิ่งที่เกินกว่ามนุษย์จะควบคุมได้ เป็นภัยที่รวมเหตุการณ์ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว และฟ้าผ่า รวมถึงภูเขาไฟระเบิด ทั้งหมดนี้ไม่เพียงแต่สร้างความยุ่งยากต่อการใช้ชีวิตของแต่ละคนเท่านั้น แต่ยังสร้างปัญหาให้กับระบบคอมพิวเตอร์ทั้งหน่วยเก็บข้อมูล สัญญาณการสื่อสารต่างๆ ภัยคุกคามสามารถแบ่งกลุ่มได้ตามรายการดังนี้

- Fire: ไฟไหม้ สร้างความเสียหายต่ออุปกรณ์ทางคอมพิวเตอร์ รวมถึงระบบสารสนเทศต่างๆ เนื่องจากควันไฟ และน้ำ ซึ่งเกิดจากการดับไฟของนักดับเพลิง ภัยจากไฟไหม้สามารถบรรเทาได้ด้วยการทำประกันอุบัติภัย เพื่อเป็นการลดความเสียหายที่เกิดขึ้นต่อทรัพย์สิน และชีวิต หรือทำประกันภัยธุรกิจ หากธุรกิจต้องหยุดดำเนินกิจการ
- Flood: น้ำท่วม เป็นสาเหตุโดยตรงที่สร้างความเสียหายต่อระบบสารสนเทศ หรือในส่วนของอาคารระบบสารสนเทศ น้ำท่วมทำให้การเข้าใช้อาคารสถานที่ หรือในส่วนการทำงานของระบบสารสนเทศติดขัด ภัยคุกคามนี้สามารถบรรเทาได้ด้วยการทำประกันอุทกภัย หรือประกันภัยธุรกิจ
- Earthquake: แผ่นดินไหว เกิดจากการเคลื่อนตัวของเปลือกโลกกะทันหัน เป็นความเสียหายทางธรณีวิทยาจากการเกิดภูเขาไฟระเบิด แผ่นดินไหวสร้างความเสียหายต่อทุกส่วนของระบบสารสนเทศ บ่อยครั้งสร้างความเสียหายกับอาคารเป็นการขัดขวางการเข้าใช้ระบบสารสนเทศ สามารถบรรเทาภัยคุกคามนี้ได้ด้วยการทำประกันภัยพิเศษ หรือ การประกันภัยธุรกิจ ทั้งนี้จะเลือกรูปแบบใดขึ้นอยู่กับการกำหนดนโยบายที่ต่างกัน
- Lightning: ฟ้าแลบ เป็นกระแสไฟฟ้าทางธรรมชาติที่ถูกปลดปล่อยออกมารบกวนคลื่นวิทยุ ฟ้าผ่าสร้างความเสียหายต่อระบบสารสนเทศ หรือ ส่วนของการจ่ายไฟ ทำให้ไฟดับ หรือ สร้างปัญหาในการใช้สถานที่ทำงานเนื่องจากไม่มีกระแสไฟฟ้า หรือ สร้างความยุ่งยากในการปฏิบัติงาน
- Landslide or mudslide: แผ่นดินถล่ม หรือ โคลนถล่ม เกิดจากดินและหินจำนวนมากไหลจากที่สูง สร้างความเสียหายต่อระบบสารสนเทศ ทั้งในส่วนของการเข้าใช้อาคารสถานที่และการเข้าใช้ระบบสารสนเทศ ซึ่งภัยคุกคามนี้สามารถบรรเทาความเสียหายได้ด้วยการทำประกันภัย หรือ การประกันภัยธุรกิจ
- Tornado or severe windstorm: พายุทอร์นาโด หรือ พายุที่มีความรุนแรงสูง เกิดจากความแปรปรวนของอากาศเป็นพายุหมุนจากจุดศูนย์กลางขนาดเล็กเพียงไม่กี่หลา ขยายความรุนแรงเพิ่มขึ้นเป็นหลายไมล์ และเป็นลมพายุที่มีความเร็วในการทำลายสูง โดยมี

รูงทรงกรวยตั้งสูงขึ้นไปยังท้องฟ้า พายุนี้สามารถสร้างความเสียหายต่อระบบสารสนเทศ ทั้งในส่วนของการเข้าใช้อาคารสถานที่ และการเข้าใช้ระบบสารสนเทศ ซึ่งภัยคุกคามนี้สามารถบรรเทาความเสียหายได้ด้วยการทำประกันภัย หรือ การประกันภัยธุรกิจ

- Hurricane or typhoon: พายุเฮอร์ริเคน หรือ พายุไต้ฝุ่น คือ พายุหมุนเขตร้อน เกิดขึ้นในแถบมหาสมุทรแอตแลนติก หรือ ทะเลคาริบเบียน หรือ แถบตะวันออกของมหาสมุทรแปซิฟิก(ไต้ฝุ่น) จากจุดศูนย์กลางพายุสามารถเคลื่อนตัวไปทางทิศเหนือ ทิศตะวันตกเฉียงเหนือ หรือ ทิศตะวันออกเฉียงเหนือ และพายุยังก่อให้เกิดฝนตกอย่างหนัก หากจุดศูนย์กลางของพายุติดชายฝั่งทะเลมักจะทำให้น้ำท่วมในพื้นที่นั้นๆ โดยพายุนี้สามารถสร้างความเสียหายต่อระบบสารสนเทศ ทั้งในส่วนของการเข้าใช้อาคารสถานที่ และการเข้าใช้ระบบสารสนเทศ ซึ่งภัยคุกคามนี้สามารถบรรเทาความเสียหายได้ด้วยการทำประกันภัย หรือ การประกันภัยธุรกิจ
- Tsunami: เป็นคลื่นขนาดใหญ่ เกิดจากแผ่นดินไหว หรือ เกิดการปะทุของภูเขาไฟใต้ทะเล ซึ่งเหตุการณ์นี้สามารถสร้างความเสียหายต่อระบบสารสนเทศ ทั้งในส่วนของการเข้าใช้อาคารสถานที่ และการเข้าใช้ระบบสารสนเทศ ซึ่งภัยคุกคามนี้สามารถบรรเทาความเสียหายได้ด้วยการทำประกันภัย หรือ การประกันภัยธุรกิจ
- Electrostatic discharge (ESD): การปะทุของไฟฟ้าสถิต โดยไฟฟ้าสถิต และESD สร้างความรำคาญ อย่างไรก็ตามเมื่อเราเดินบนพรมจะเกิดไฟฟ้าสถิตทำให้เรารู้สึกเหมือนถูกไฟดูดเล็กน้อย แต่การปะทุของไฟฟ้าสถิตสามารถทำลายหรือสร้างความเสียหายอย่างมาก เมื่อมีการรวมกันก่อให้เกิดการจุดติดไฟได้ง่ายกับส่วนประกอบของวงจรอิเล็กทรอนิกส์ ไฟฟ้าสถิตทำให้พื้นที่มีประจุดูดฝุ่นละอองไว้ในห้องที่สะอาด หรือ ทำให้ผลิตภัณฑ์เกิดไฟฟ้าสถิต มูลค่าความเสียหายจากอุปกรณ์อิเล็กทรอนิกส์ และการหยุดให้บริการมีตั้งแต่ไม่กี่เซนต์ไปจนถึงหลายล้านดอลลาร์ สำหรับอันตรายที่จะเกิดกับระบบอิเล็กทรอนิกส์ ซึ่งความเสียหายในกระบวนการผลิตทำให้เสียเวลา เนื่องจากผลกระทบของ ESD นั้นมีนัยสำคัญ ถึงแม้ว่า ESD จะดูว่าไม่เป็นภัยคุกคาม แต่สามารถสร้างความยุ่งยากให้กับระบบสารสนเทศ ซึ่งปัญหานี้ไม่สามารถทำประกันภัยคุ้มครองความเสียหาย หรือ การทำประกันภัยธุรกิจ
- Dust contamination: การปนเปื้อนจากฝุ่น สภาพแวดล้อมบางอย่างมิได้เป็นผลดีต่ออุปกรณ์ฮาร์ดแวร์ของระบบสารสนเทศ เพราะฝุ่นทำให้อายุการใช้งานของระบบสารสนเทศสั้นลง หรือ เป็นเหตุให้เครื่องคอมพิวเตอร์หยุดการทำงาน ภัยคุกคามนี้เป็นปัญหาธรรมดาในการปฏิบัติงาน

เนื่องจากภัยคุมคามทางธรรมชาติไม่อาจที่จะหลีกเลี่ยงได้ องค์กรต้องเพิ่มการควบคุมที่จะจำกัดความเสียหาย และต้องวางแผนกับความไม่แน่นอนสำหรับการปฏิบัติงานอย่างต่อเนื่อง เช่น แผนการกู้ข้อมูล วางแผนอย่างต่อเนื่อง และแผนการรับมือกับเหตุการณ์ที่อาจเกิดขึ้นโดยบังเอิญ เพื่อจำกัดความเสียหายจากภัยคุกคามเหล่านี้

9. คุณภาพของบริการ (Deviations in Quality of Service)

ระบบสารสนเทศขององค์กรจะประสบความสำเร็จได้นั้นต้องได้รับการสนับสนุนจากระบบอื่นๆ ร่วมด้วย เช่น โรงไฟฟ้า เครือข่ายโทรคมนาคม ผู้จัดจำหน่าย ผู้ให้บริการ เจ้าหน้าที่ดูแลรอบค่ำ ซึ่งระบบสนับสนุนเหล่านี้อาจหยุดชะงักได้หากเกิดพายุ พนักงานป่วย หรือเหตุฉุกเฉิน ภัยคุกคามเหล่านี้ทำการโจมตี ทำให้คุณภาพการให้บริการคลาดเคลื่อน เช่น ถ้ารถขุดเจาะถูกสายไฟเบอร์ออฟติกที่มาจาก ISP องค์กรควรเตรียมการสำรองข้อมูลทั้งการเชื่อมต่อผ่านระบบเครือข่าย และการบริการ แต่ต้องรีบดำเนินการในส่วนของความเร็วในการรับ-ส่งข้อมูลขององค์กร เนื่องจากเป็นสิ่งสำคัญสำหรับการให้บริการที่สมบูรณ์ ความผิดปกติจากการให้บริการอินเตอร์เน็ต การติดต่อสื่อการ และเครื่องจ่ายไฟสามารถส่งผลกระทบอย่างรวดเร็วต่อข้อมูล และสร้างความเสียหายต่อระบบได้

Internet Service Issues

องค์กรในปัจจุบันนิยมการใช้อินเตอร์เน็ตในการค้นหาและเข้าถึงข้อมูลบนอินเตอร์เน็ต เพื่อช่วยในการปฏิบัติงาน ซึ่งผู้ให้บริการอินเตอร์เน็ตจะต้องให้ความสำคัญกับ การก่อวินาศกรรมของข้อมูลข่าวสาร ในหลายองค์กรพนักงานขาย หรือ พนักงานขายทางโทรศัพท์สามารถทำงานจากสถานที่ซึ่งอยู่ไกลกันได้

องค์กรที่มีเว็บไซต์จะมีผู้ให้บริการเว็บโฮสติ้งดูแลเว็บให้ ซึ่งเว็บโฮสติ้งจะรับผิดชอบกับบริการอินเตอร์เน็ตทั้งหมด รวมถึงฮาร์ดแวร์ และซอฟต์แวร์ระบบที่เกี่ยวกับการทำงานของเว็บไซต์ ผู้ให้บริการเว็บโฮสติ้งจะมีข้อตกลงเกี่ยวกับระดับการให้บริการขั้นพื้นฐานที่ควรรู้ คือ **Service Level Agreement (SLA)** ผู้ให้บริการจะขาดพันธะสัญญาในการให้บริการไม่ได้ และพันธะสัญญาควรครอบคลุมความเสียหายที่ยังไม่เกิดขึ้นกับลูกค้า แต่เป็นเรื่องยากหากจะคลอบคลุมความเสียหายที่เกิดจากช่วงที่ไม่มีกระแสไฟฟ้า

บริการด้านการสื่อสารและผู้ให้บริการอื่น ๆ (Communications and other Service Provider Issues)

บริการสาธารณูปโภคที่ดีต่อองค์กร บริการเหล่านี้คือ โทรศัพท์ น้ำประปา รถเก็บขยะ ระบบส่งสัญญาณโทรศัพท์ด้วยสายเคเบิล ก๊าซธรรมชาติ และการดูแลทรัพย์สิน โดยบริการเหล่านี้มีผลต่อความเสียหายขององค์กรได้ องค์กรมีความต้องการน้ำไปจนถึงระบบเครื่องทำความเย็น เพื่อความมสะดวกในการปฏิบัติงาน

ปัญหากระแสไฟฟ้า (Power Irregularities)

ความผิดปกติของไฟฟ้าเป็นสิ่งที่เกิดขึ้นได้ทุกวัน เช่น ไฟเกิน ไฟตก และไฟดับ ซึ่งองค์กรต้องเตรียมแนวทางในการแก้ปัญหาไฟฟ้าสำหรับอุปการณ์ระบบสารสนเทศ ในสหรัฐจะใช้ไฟฟ้าที่ 120 โวลต์ , 60 cycle โดยปกติจะมีกระแสไฟที่ 15 และ 20 แอมป์

เมื่อแรงดันไฟฟ้าที่ระดับ **spike** (แรงดันไฟเพิ่มขึ้นชั่วขณะ) หรือ **surge** (แรงดันไฟเพิ่มขึ้นอย่างรุนแรง) ซึ่งแรงดันไฟที่เพิ่มขึ้นสร้างความเสียหายให้กับอุปกรณ์ต่างๆได้ การขาดแคลนไฟฟ้าเกิดจากการจ่ายไฟไม่ทั่วถึง

เมื่อแรงดันไฟลดลง(sag) หรือ ไฟตก คือแรงดันไฟลดลง เป็นสาเหตุให้ระบบปิดการทำงาน หรือ รีเซตระบบใหม่ทำให้เกิดการขัดข้องในการใช้ระบบ ซึ่งส่งผลต่ออุปกรณ์อิเล็กทรอนิกส์ โดยเฉพาะอุปกรณ์เครือข่าย คอมพิวเตอร์ และระบบคอมพิวเตอร์พื้นฐานเกิดความเสียหาย ควรจะจัดการควบคุมการจ่ายกระแสไฟให้มีคุณภาพ โดยเครื่อง UPS สามารถป้องกันเรื่องแรงดันไฟฟ้าไม่คงที่ได้ เช่น ไฟตก ไฟเกิน และไฟดับ

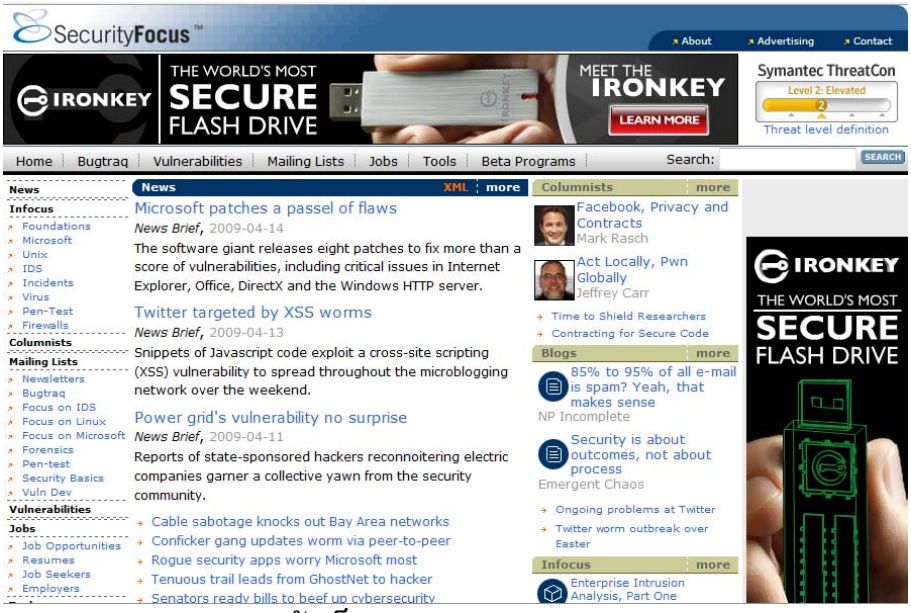
10. ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical Hardware Failures or Errors)

ความล้มเหลวทางเทคนิคของฮาร์ดแวร์ หรือความผิดพลาดที่การผลิตอุปกรณ์เกิดข้อบกพร่อง เป็นเหตุให้การทำงานของอุปกรณ์ภายนอกของระบบไม่เป็นไปอย่างที่คิด ส่งผลให้การบริการไม่น่าไว้วางใจ หรือใช้ประโยชน์ไม่ได้ บางครั้งความผิดปกติของจอคอมพิวเตอร์ อุปกรณ์ต่อพ่วงอื่นๆ หากเสียหายจะไม่สามารถนำกลับมาใช้งานได้ดังเดิม

11. ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical Software Failures or Errors)

การเขียนโค้ดคอมพิวเตอร์ส่วนมาก มีการตรวจสอบจุดบกพร่อง วิเคราะห์ข้อผิดพลาดทั้งหมดก่อนที่จะจำหน่าย ในบางครั้งจะตรวจสอบซอฟต์แวร์และฮาร์ดแวร์ร่วมกัน จะแสดงจุดบกพร่องใหม่ๆได้ ความล้มเหลวจะเกิดขึ้นหากไม่มีการตรวจสอบจุดบกพร่องต่างๆ บางครั้งการตรวจสอบอาจจะไม่พบข้อผิดพลาด แต่โปรแกรมเมอร์ส่วนมากจะสร้างช็อตคัทไว้ซึ่งอาจจะเป็นเหตุให้เกิดความเสียหายได้ เนื่องจากช็อตคัทสามารถเข้าสู่ตัวโปรแกรมได้โดยปราศจากการตรวจเช็คความปลอดภัยตั้งแต่เริ่มต้น เป็นการฝ่าฝืนแนวทางในการรักษาความปลอดภัย

ข้อผิดพลาดของซอฟต์แวร์ถูกรวบรวมเป็นเอกสารไว้ที่เว็บไซต์ http://www.securityfocus.com ซึ่งมีข้อมูลล่าสุดของการป้องกันความมั่นคงปลอดภัย รวมถึงเอกสารสำคัญที่บอกถึงข้อบกพร่องในอดีตได้ละเอียดที่สุด



รูปแสดง หน้าเว็บ http://www.securityfocus.com/

12. เทคโนโลยีล้าสมัย (Technological Obsolescence)

โครงสร้างพื้นฐานที่ล้าสมัยทำให้ระบบไม่ปลอดภัย และไม่น่าไว้ใจ ผู้บริหารควรจะรู้ว่าเมื่อเทคโนโลยีล้าสมัย ส่งผลถึงความเสี่ยงด้านความมั่นคงของข้อมูลอาจพบกับภัยคุมคามได้ ผู้บริหารควรมีการวางแผนกลยุทธ์ รวมถึงการวิเคราะห์ในการเลือกใช้เทคโนโลยีในปัจจุบัน ตามหลักควรมีการวางแผนที่เหมาะสม ในการป้องกันเทคโนโลยีล้าสมัย เมื่อพบว่าเทคโนโลยีล้าสมัยต้องจัดการทันที โดยผู้เชียวชาญด้านเทคโนโลยีได้กำหนดลักษณะสิ่งที่น่าจะเป็นความล้าสมัย

ปัจจุบัน Symantec เลิกสนับสนุนซอฟต์แวร์แอนติไวรัสเวอร์ชันเก่า และให้การสนับสนุนผลิตภัณฑ์อย่างต่อเนื่องด้วยการอัพเกรดซอฟต์แวร์ให้ทันที ถ้าในองค์กรมีเจ้าหน้าที่ IT ที่เชียวชาญจะมีการจัดการอัพเกรดซอฟต์แวร์ที่ล้าสมัยทันที ซึ่งเป็นการลดค่าใช้จ่ายขององค์กร

ATTACKS

การโจมตีเป็นการกระทำเพื่อให้เกิดความไม่มั่นคงและเป็นอันตรายต่อการควบคุมระบบคอมพิวเตอร์ โดยเป้าหมายของการโจมตีเพื่อสร้างความเสียหายหรือการขโมยข้อมูลที่สำคัญขององค์กร ในส่วนนี้จะเป็นการอธิบายแต่ละประเภทของการโจมตีระบบที่สำคัญ ๆ

Malicious Code

การโจมตีแบบ Malicious Code จะประกอบไปด้วยไวรัส, เวิร์มและไวรัสโทรจัน เพื่อจุดประสงค์ในการทำลายระบบหรือการขโมยข้อมูล ซึ่งในตัวโปรแกรมไวรัสเหล่านี้ อาจจะมีเทคนิคการโจมตี 6 ประเภทรวมอยู่ด้วยกัน เพื่อสร้างความหลากหลายในการโจมตีไปที่จุดอ่อนของเครื่องเป้าหมายและทำให้ไวรัสแพร่กระจายได้อย่างรวดเร็ว ตัวอย่างเช่น ไวรัส Nimda มีการทำงานที่ซับซ้อนและใช้เทคนิคหลายอย่างผสมกัน จึงทำให้สามารถแพร่กระจายได้อย่างรวดเร็ว ตามรายงาน

ของบริษัท TureSecure ได้เปิดเผยข้อมูลด้านสถิติระบุว่า ไวรัส Nimda แพร่กระจายไปยัง 14 ประเทศ โดยใช้เวลาน้อยกว่า 25 นาทีเท่านั้น

ตารางแสดงเทคนิคในการโจมตีและแพร่กระจายไวรัส

Vector	รายละเอียด
IP Scan and Attack	ใช้เครื่องที่ติดไวรัสในการสแกนค้นหาหมายเลขไอพี และดูว่าเป้าหมายไหนที่มีการป้องกันที่อ่อนแอ แล้วส่งไปให้กับตัวของผู้บุกรุก (Hacker)
Web browsing	ถ้าเครื่องที่ติดไวรัส และสามารถเข้าถึงเว็บเพจได้ จะทำให้ไฟล์ที่เกี่ยวกับเว็บ (.html, .asp, .cgi อื่นๆ) ตัวผู้ใช้เข้าถึงเว็บไซด์ดังกล่าวก็จะทำให้ติดไวรัสไปด้วย
Virus	เครื่องที่ติดไวรัส ตัวไวรัสสามารถที่จะคัดลอกตัวเองจะทำให้ไฟล์ประเภท EXE และ Script File ต่างๆ ติดไวรัสได้
Unprotected shares	ใช้ความไม่มั่นคงของระบบ Files System โดยเครื่องที่ติดไวรัสจะทำการคัดลอกไวรัสไปยังส่วนต่างๆ ที่สามารถเข้าถึงได้
Mass mail	เป็นการส่งอีเมล์ ไปยังที่อยู่ของผู้รับที่เครื่องที่ติดไวรัสรู้จัก ใครที่ได้รับอีเมล์และเปิดอ่านก็จะทำให้โปรแกรมไวรัสทำงานทันทีและทำให้เครื่องติดไวรัส
Simple Network Management Protocol (SNMP)	SNMP เป็นโปรโตคอลที่ใช้สำหรับการเฝ้าสังเกตเครือข่ายและอุปกรณ์ในเครือข่าย โดยโปรแกรมในการโจมตีจะเข้าไปควบคุมอุปกรณ์ ส่วนมากผู้ผลิตจะทำการปิดจุดอ่อนในส่วนนี้ด้วยการอัพเกรดตัวซอฟต์แวร์ของอุปกรณ์

Hoaxes

ส่วนมากมักจะอยู่ในรูปแบบการหลอกลวงเพื่อทำการโจมตีคอมพิวเตอร์ โดยผู้โจมตีจะทำการส่งข้อความที่มีความน่าเชื่อถือ ถ้าผู้ที่ได้รับข้อความปฏิบัติตามอาจจะทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ เช่น การให้ลบไฟล์ข้อมูลที่จำเป็นของระบบปฏิบัติการโดยหลอกว่าเป็นไวรัสคอมพิวเตอร์ ทำให้ระบบปฏิบัติการทำงานผิดปกติ เป็นต้น นอกจากนี้ผู้ได้รับข้อความจะทำการส่งผ่านข้อความที่ตนเองได้รับไปให้กับเพื่อนของตนเอง เหมือนกับจดหมายลูกโซ่

Back Doors

เป็นช่องโหว่ในการรักษาความปลอดภัยที่ถูกทิ้งไว้โดยผู้ออกแบบระบบหรือทีมงานบำรุงรักษาระบบ ซึ่งผู้บุกรุกจะใช้ช่องโหว่นี้หรือ Back Door ในการเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ บางครั้งเรียกว่า Trapdoor ซึ่ง Trapdoor เป็นอะไรที่ป้องกันได้ยาก เพราะว่าบ่อยครั้ง

โปรแกรมเมอร์เป็นผู้ที่ทิ้งช่องโหว่นี้ไว้เอง เพื่อให้สามารถเข้าถึงระบบโดยไม่ต้องผ่านระบบความปลอดภัยของระบบ จุดประสงค์เพื่ออำนวยความสะดวกต่อโปรแกรมเมอร์หรือผู้ตรวจสอบระบบ (Audit) ในการเข้าถึงระบบได้ง่ายและรวดเร็ว

Password Crack

เป็นความพยายามในการคำนวณแบบย้อนกลับเพื่อให้ได้มาซึ่งรหัสผ่าน (Password) บางครั้งเรียกกระบวนการนี้ว่า Cracking โดยจะทำการคัดลอก Security Account Manager (SAM) ซึ่งภายในไฟล์ SAM จะมีส่วนประกอบของวิธีการของการคำนวณรหัสผ่านของผู้ใช้ ซึ่งวิธีการคำนวณนั้นใช้ อัลกอริทึ่ม (Algorithms) แบบเดียวกันในการคำนวณหารหัสผ่านและในการเปรียบเทียบถ้าผลลัพธ์ในการคำนวณออกมาเหมือนกัน รหัสผ่านก็จะถูกถอดรหัสออกมา

Brute Force

เป็นโปรแกรมที่ผู้บุกรุกใช้สำหรับเดารหัสที่เป็นไปได้ที่เกิดขึ้นจากการสร้างรหัสผ่าน (Password) วิธีการนี้เรียกว่าการโจมตีแบบ Brute Force หรือบางครั้งก็เรียกว่า Password Attack เช่นสมมุติว่ารหัสผ่านที่เป็นไปได้ของระบบเป็นตัวอักษรภาษาอังกฤษพิมพ์เล็กจำนวน 4 ตัว ผู้บุกรุกก็พยายามล็อกอินเข้าสู่ระบบโดยใช้รหัสผ่านที่เป็นไปได้ทั้งหมดจากการผสมคำ ในกรณีนี้ รหัสผ่านที่เป็นไปได้คือ 26x26x26x26 ตัว ซึ่งถ้าตั้งรหัสผ่านมีการผสมกันระหว่างตัวอักษรทั้งตัวเล็ก ตัวใหญ่ ตัวเลขและเครื่องหมายต่างๆ จะทำให้คำที่เป็นไปได้ทั้งหมดมีจำนวนมากขึ้น ดังนั้นหากผู้บุกรุกใช้วิธีนี้ในการเดารหัสผ่านก็จะใช้เวลานานยิ่งขึ้น

สำหรับวิธีการโจมตีแบบ Brute Forceนั่นจะประสบความสำเร็จไม่บ่อยครั้งนัก เนื่องจากระบบความปลอดภัยของระบบ ได้มีการจำกัดจำนวนครั้งในการใส่รหัสผ่านเอาไว้

Dictionary

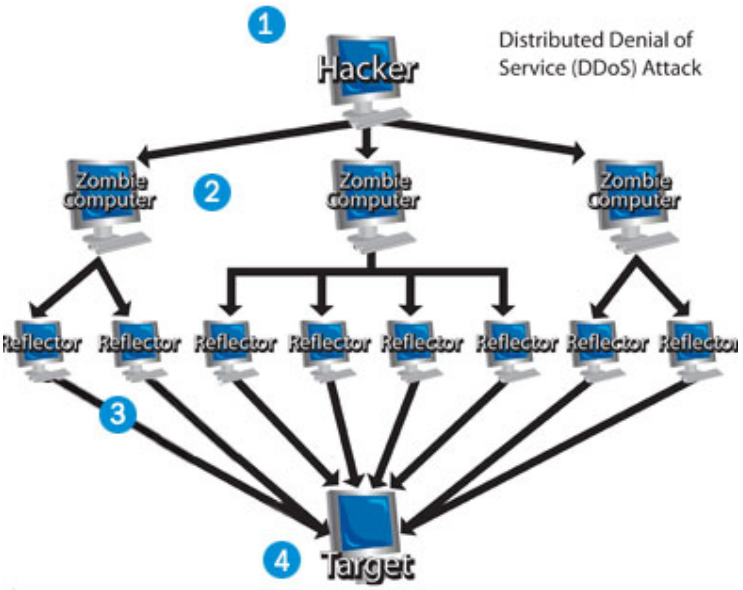
วิธีการโจมตีแบบ Dictionary Attack จะมีความแตกต่างจาก Brute Force โดยโปรแกรมจะทำการเลือกคำที่มีอยู่ในดิกชันนารี่มาใช้ในการสร้างรหัสผ่าน (Password) วิธีการป้องกันการโจมตีด้วย Dictionary Attack โดยการไม่อนุญาตให้ใช้คำที่มีอยู่ในดิกชันนารี่มาใช้เป็นรหัสผ่าน หรือใช้ตัวเลขหรืออักขระพิเศษเพิ่มเข้าไปในรหัสผ่าน ก็จะทำให้การโจมตีด้วย Dictionary Attack ลดประสิทธิภาพลงไป

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

การโจมตีด้วยวิธี Denial-of-Service (Dos) เป็นการโจมตีที่ผู้โจมตีจะส่งข้อมูลแพ็กเกตจำนวนมหาศาลไปยังที่เครื่องเป้าหมาย จนทำให้เครื่องเป้าหมายทำงานหนัก จุดประสงค์ของการโจมตีเพื่อทำให้ระบบล่มหรือไม่สามารถทำงานได้ตามปกติ

การโจมตีด้วยวิธี Distributed denial-of-service (DDoS) เป็นการโจมตีเครื่องเป้าหมายจากหลายๆ แห่งในเวลาพร้อมๆ กัน วัตถุประสงค์ของการโจมตีเหมือนกันกับ DoS คือเพื่อหยุดการทำงานของระบบ เป็นเหตุให้ระบบไม่สามารถใช้งานได้ตามปกติ ซึ่งการป้องกันการโจมตีประเภทนี้ทำได้ยาก และสร้างความเสียหายเป็นอย่างมาก

การโจมตีด้วยเวิร์ม (Worm) ที่ชื่อว่า “My Doom” ในระหว่างปี 2004 ซึ่งเป็นการโจมตีด้วยวิธี Distributed denial-of-service (DDoS) โดยมีวัตถุประสงค์เพื่อโจมตี www.sco.com (เว็บไซต์ของบริษัทผู้จัดจำหน่ายระบบปฏิบัติการ UNIX) การโจมตีเกินขึ้นระหว่างวันที่ 1 กุมภาพันธ์ 2004 – วันที่ 12 กุมภาพันธ์ 2004 เหตุผลของผู้โจมตีเพื่อเป็นโต้ตอบกลับบริษัท SCO ที่มีวัตถุประสงค์มุ่งร้ายต่อ Community ของโอเพ่นซอร์สระบบปฏิบัติการลีนุกซ์



รูปแสดง Distributed Denial of Service Attack (DDoS)

แหล่งอ้างอิง: http://computer.howstuffworks.com/zombie-computer3.htm

Spoofing

Spoofing เป็นเทคนิคที่ใช้เพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาตได้ โดยการส่งข้อความปลอมๆ ที่ดูเหมือนจะจากเครื่องที่ได้รับการเชื่อถือ (Trusted host) อาศัยการปลอม IP Address ของเครื่องนั้น วิธีการได้มาซึ่ง IP Address ที่มีความน่าเชื่อถือของผู้บุกรุกก็มีอยู่ด้วยกันหลายวิธีด้วยกัน ปัจจุบันเราเตอร์และไฟร์วอลล์รุ่นใหม่ๆ ได้มีการจัดการป้องกันการโจมตีแบบ IP Spoofing

Man-in-the-Middle

เป็นที่รู้จักกันดีของวิธีการโจมตีแบบ Man-in-the-Middle หรือ TCP hijacking attack คือผู้บุกรุกจะนำแพ็กเกจที่วิ่งอยู่บนเครือข่าย มาทำการแก้ไข เพิ่มข้อมูล ปลอมแปลงข้อมูลและทำการส่งกลับไปยังเครือข่ายเหมือนเดิม ถือว่าเป็นหนึ่งในประเภทของการโจมตีแบบ IP Spoofing

สำหรับวิธีการขัดขวางการถูกโจมตีแบบ TCP hijacking คือการเข้ารหัสด้วยการแลกเปลี่ยนคีย์ระหว่างผู้รับและผู้ส่ง ใช้ในการเข้ารหัสและถอดรหัสข้อมูล เพื่อป้องกันการถูกเข้าถึงข้อมูลจากบุกรุก หรือถ้าผู้เข้าถึงข้อมูลก็สามารถทราบได้ว่าข้อมูลถูกเปลี่ยนแปลง

Spam

เป็นอีเมล์ที่เราไม่ต้องการ จุดประสงค์ของผู้ส่ง Spam Mail เพื่อต้องการโฆษณาและบริการต่างๆ สำหรับ Spam Mail จะสร้างความรำคาญให้กับผู้รับอีเมล์มากกว่าจุดประสงค์เพื่อการโจมตี แต่ในเดือนมีนาคม ปี 2002 มีรายงานว่ามีการแนบไวรัสมากับ Spam Mail ด้วย

หลายๆ บริษัทพยายามที่จะป้องกัน Spam Mail โดยการที่ใช้เทคโนโลยีในการคัดกรองอีเมล์ แต่ก็มีบางบริษัทที่ใช้วิธีแบบง่ายๆ โดยให้ผู้ใช้ลบอีเมล์ที่ไม่ต้องการออกจากระบบอีเมล์ของบริษัทด้วย

Mail Bombing

เป็นการโจมตีอีกรูปแบบหนึ่งจากการใช้อีเมล์มีลักษณะการโจมตีที่คล้ายกับ DoS (Denial-of-Service) เรียกว่า Mail Bomb เป็นการที่ผู้โจมตีทำการส่งอีเมล์จำนวนมหาศาลไปยังเครื่องเป้าหมายเพื่อจุดประสงค์ทำให้ระบบอีเมล์ล่มไม่สามารถทำงานได้ตามปกติ

Sniffers

Sniffer เป็นโปรแกรมหรืออุปกรณ์ที่คอยดักจับข้อมูลที่วิ่งอยู่บนระบบเครือข่าย Sniffer สามารถถูกนำไปใช้ในด้านที่ดีและไม่ดี ด้านที่ดีคือ Sniffer สามารถช่วยในการบริหารจัดการเครือข่าย เช่นใช้ในการวิเคราะห์ปัญหาความผิดพลาดของระบบเครือข่าย ส่วนในการนำไปใช้ในด้านที่ไม่ดีคือการใช้เพื่อการขโมยข้อมูล ซึ่งการใช้ Sniffer โดยไม่ได้รับอนุญาตของผู้บุกรุก จะเป็นอันตรายต่อความปลอดภัยของเครือข่ายอย่างมาก เพราะว่าหลายๆ ระบบและผู้ใช้จะมีการส่งข้อมูลระหว่างกันโดยใช้เครือข่ายภายใน ซึ่งจะไม่มีการเข้ารหัสข้อมูล ก็จะทำให้โปรแกรม Sniffer สามารถมองเห็นข้อมูลได้ทั้งหมด ไม่ว่าจะเป็นรหัสผ่านต่างๆ และข้อมูลที่อยู่ภายในเอกสาร

Social Engineering

Social Engineering เป็นเทคนิคการใช้ทักษะในการโน้มน้าวให้ผู้อื่นยอมเปิดเผยข้อมูลส่วนตัวหรือข้อมูลสำคัญอื่นๆ ให้กับผู้โจมตี ยกตัวอย่างในกรณีที่ผู้โจมตีทราบชื่อของ CIO ของบริษัท แล้วทำแอบอ้างเป็น CIO เพื่อทำการหลอกลวงเพื่อสอบถามข้อมูลที่ผู้โจมตีต้องการจากพนักงานของบริษัท

Phishing

การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ (Email Spoofing) และทำการสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ

สามารถทำได้โดยการขโมยหรือนำเครื่องหมายหรือสัญลักษณ์ตลอดจนรูปลักษณ์ของธนาคารหรือสถาบันการเงินที่มีชื่อเสียง และบัตรเครดิตประเภทต่างๆของผู้ประกอบการ การให้สินเชื่อทางอินเตอร์เน็ต มาประกอบเข้ากับการหลอกลวงเหยื่อหรือผู้ใช้ให้เปิดเผยข้อมูล ซึ่งมีการประเมินเบื้องต้นว่า การโจมตีในรูปแบบของ Phishing สามารถหลอกให้เหยื่อร้อยละ 5 ของทั้งหมด เปิดเผยข้อมูลที่ต้องการ นอกจากนี้ ผู้โจมตี (Hacker หรือ Spammer) ยังใช้ยุทธวิธีการหลอกลวงแบบ Social Engineering ประกอบเพิ่มเติม เพื่อให้มีความน่าเชื่อถือยิ่งขึ้น เช่น การหลอกลวงชื่ออี-เมล์ เป็นต้นว่า

เป็นเรื่องด่วนจากธนาคาร การหลอกลวงว่าบัญชีที่ใช้งานจะหมดอายุ การเสนอสินค้าที่มีดอกเบี้ยต่ำต่างๆ เป็นต้น

Pharming

การโจมตีด้วยวิธีการ Pharming นี้ เหยื่อจะสังเกตได้ยากมาก หรือเรียกได้ว่าแทบไม่รู้ตัวเลยก็ว่าได้ เพราะ URL ที่เข้าไปก็เหมือนกับของ Web Site จริงทุกประการ แต่เป็นกลลวงที่ระบบ DNS ทำให้เหยื่อเกิดความเข้าใจผิด

Timing Attack

การโจมตีแบบ Timing Attack เป็นการเข้าไปทำการสำรวจภายในหน่วยความจำของตัวเว็บบราวเซอร์ (Web Browser) และทำการส่งคุกกี้ (Cookies) ที่มีวัตถุประสงค์ร้ายเข้าไปยังเครื่องเป้าหมาย โดยตัวคุกกี้นั่นจะทำการเก็บรวบรวมข้อมูล เพื่อให้ทราบว่าจะสามารถเข้าสู่เว็บไซต์ที่ป้องกันด้วยรหัสผ่านได้อย่างไรการโจมตีอีกแบบที่มีชื่อเหมือนกันจะเป็นการโจมตีที่เกี่ยวข้องกับกับการดักข้อมูลที่ใช้สำหรับการถอดรหัสข้อมูล ได้แก่กุญแจที่ใช้ในการถอดรหัสและอัลกอริทึ่มที่ใช้ในการเข้ารหัสข้อมูล

การพัฒนาซอฟต์แวร์ให้มีความปลอดภัย (Secure Software Development)

ระบบประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย ข้อมูล การประมวลผลและผู้ใช้ระบบ ในบทนี้จะพูดถึงเรื่องความปลอดภัยของข้อมูล ซึ่งมีต้นเหตุมาจากส่วนของซอฟต์แวร์ระบบ ระบบความปลอดภัยต้องการความมั่นคงหรืออย่างน้อยที่สุดจะต้องปลอดภัย ผู้พัฒนาระบบและซอฟต์แวร์เป็นผู้ที่มีความสามารถในการใช้ขั้นตอนวิธี เช่น วงจรการพัฒนาระบบ (SDLC) องค์กรจำนวนมากให้ความสำคัญสำหรับการวางแผนความปลอดภัย ในขั้นตอนของการพัฒนาระบบ สำหรับการสร้างระบบและในขั้นตอนของการปฏิบัติงานสำหรับการพัฒนาซอฟต์แวร์ให้มีรูปแบบความปลอดภัย วิธีการพัฒนาซอฟต์แวร์ที่มีชื่อเสียงคือการประกันซอฟต์แวร์ (SA)

การประกันซอฟต์แวร์และความรู้พื้นฐานที่สำคัญของการประกันซอฟต์แวร์ (Software Assurance and the SA Common Body of Knowledge)

ที่กล่าวถึงในบทที่ 1 องค์กรส่วนมากต้องการความปลอดภัยในขั้นตอนของการพัฒนาระบบต้องการที่จะป้องกันปัญหาด้านความปลอดภัยก่อนที่จะเริ่มวงจรพัฒนาระบบ ในระดับชาติพยายามที่จะสร้างความรู้พื้นฐานที่สำคัญ (CBK) ที่มุ่งไปที่ความปลอดภัยของการพัฒนาซอฟต์แวร์ The US Department of Defense (DoD) ได้ออกรูปแบบการประกันซอฟต์แวร์ ซึ่งเริ่มขึ้นในปี 2003 ขั้นตอนเริ่มต้นโดย Joe Jarzombek ได้รับการรับรองและสนับสนุนจาก Department of Homeland Security (DHS) รวมลงทุนในปี 2004 แผนการเริ่มต้นทำให้เกิดสิ่งพิมพ์ ความปลอดภัยของการประกันซอฟต์แวร์ (SwA) ความรู้พื้นฐานที่สำคัญ คณะทำงานได้ร่างเอกสารจากวงการอุตสาหกรรม รัฐบาล สถานศึกษา มีรูปแบบในการสำรวจ 2 หัวข้อในการตอบคำถาม

1. อะไรเป็นกิจกรรมของวิศวะกรหรือลักษณะของกิจกรรมที่สำคัญที่ทำให้ได้ซอฟต์แวร์ที่ปลอดภัย
2. ความรู้อะไรเป็นที่ต้องการในการปฏิบัติงาน หรือ กิจกรรมที่ต้องการ

บนพื้นฐานของการค้นพบของคณะทำงานและกลุ่มของเอกสารภายนอกที่มีอยู่และมาตรฐานความปลอดภัยของการประกันซอฟต์แวร์ ความรู้พื้นฐานที่สำคัญ ที่พัฒนาแล้วและตีพิมพ์เพื่อใช้เป็นคู่มือ ในขณะที่การทำงานยังไม่ประสบความสำเร็จการยอมรับมาตรฐานที่แท้จริง หรือแม้ว่าความต้องการนโยบายของหน่วยงานภาครัฐบาล ที่สนับสนุนและให้คำแนะนำที่ดีที่กำลังพัฒนามากกว่าแอ็พพลิเคชั่นที่ปลอดภัย การค้นหา เช่น ระยะเวลาของขั้นตอนการทำงานทั้งหมดของโปรแกรม รวมถึงเรื่องทั่วๆ ไปของความไม่ปลอดภัย แนวคิดพื้นฐานและทฤษฎี จริยธรรม กฎหมายและการปกครองความต้องการซอฟต์แวร์ที่ปลอดภัย การตรวจสอบซอฟต์แวร์ที่ปลอดภัย การถูกต้องตามกฎหมายและการประเมินผล เครื่องมือและวิธีการพัฒนาซอฟต์แวร์ที่ปลอดภัย กระบวนการของซอฟต์แวร์ที่ปลอดภัย การควบคุมโครงการซอฟต์แวร์ที่ปลอดภัย การได้มาซอฟต์แวร์ที่ปลอดภัย และการสนับสนุนซอฟต์แวร์ที่ปลอดภัย

หลักการออกแบบซอฟต์แวร์ (Software Design Principles)

การพัฒนาซอฟต์แวร์ที่ดีจะต้องได้ผลลัพธ์ในขั้นสุดท้ายของผลิตภัณฑ์ ต้องเป็นไปตามคุณสมบัติของการออกแบบ ความปลอดภัยของระบบสารสนเทศต้องพิจารณาในข้อมูลเฉพาะ ปัจจุบันต้องสนใจปัจจัยอันตราย หรือสิ่งที่ไม่ถูกต้องตลอดเวลา J. H. Saltzer และ M. D. Schroeder ผู้นำในด้านการพัฒนาซอฟต์แวร์ให้คำอธิบายของการออกแบบไว้ว่า

“การป้องกันสารสนเทศในระบบคอมพิวเตอร์และประโยชน์ของกลไกการป้องกันอยู่บนความสามารถของระบบที่จะป้องกัน การละเมิดความปลอดภัยในการปฏิบัติ, การผลิตระบบที่ระดับใดๆความสามารถในการปฏิบัติได้ตามความจริงของการป้องกันทั้งหมด เช่น การกระทำที่ไม่มีสิทธิ์พิสูจน์ได้อยากลำบากที่สุด ผู้ใช้ที่มีประสบการณ์มากมีความตระหนักอย่างหนึ่ง คือการเงินของระบบการปฏิเสธผู้ใช้อื่นๆ ที่ให้สิทธิเข้าถึงกับสารสนเทศ การโจมตีที่เกี่ยวข้องจำนวนมากของความผิดปกติทั่วๆ ไปของระบบทั้งหมด ที่เห็นนั้นผู้ใช้สามารถสร้างโปรแกรมที่ไม่ได้รับการอนุญาตให้เข้าถึงสารสนเทศ แม้แต่ในการออกแบบระบบและการทำให้สำเร็จด้วยความปลอดภัยเป็นจุดประสงค์ที่สำคัญ การออกแบบและการทำให้ประสบความสำเร็จมีแนวทางหลีกเลี่ยงเจตนาบังคับการเข้าถึง การออกแบบและเทคนิคโครงสร้างอย่างเป็นระบบนั้น แยกข้อบกพร่องเป็นหัวข้อกิจกรรมมากมายของการวิจัย แต่ไม่ใช่วิธีการทั้งหมดที่สามารถนำไปปรับใช้ได้ตรงกับโครงสร้างส่วนมากของจุดประสงค์ทั่วไปของระบบที่มีอยู่

รายการที่แน่ชัดเกี่ยวกับการพัฒนาซอฟต์แวร์ในยุคก่อนศตวรรษที่ 21 แต่เกิดขึ้นจริงย้อนกลับไปก่อนปี 1975 ความปลอดภัยของสารสนเทศและการประกันซอฟต์แวร์ที่เหมาะสมเกี่ยวข้องกับความสำเร็จขององค์กร ในบทความนี้หัวข้อที่ให้ความเข้าใจเกี่ยวกับทฤษฎีที่เกิดขึ้นในปัจจุบัน ข้อปฏิบัติที่ปลอดภัย

a. กลไกทางเศรษฐกิจ : ดำเนินการออกแบบให้ง่ายๆ และเล็กเท่าที่เป็นไปได้
b. อุปกรณ์ป้องกันเป็นตัวเลือกโดยอัตโนมัติ : พื้นฐานการตัดสินใจการเข้าใช้งานที่ได้รับการอนุญาตแทนการยกเว้น
c. การอยู่ตรงกลางทั้งหมด : ทุกครั้งที่ต้องการเข้าใช้งาน ทุกจุดประสงค์ จะต้องตรวจสอบสิทธิ์
d. การออกแบบเปิดกว้าง : การออกแบบไม่ควรจะเป็นความลับ แต่จะต้องขึ้นอยู่กับการควบคุมในเรื่องการป้อนข้อมูลหรือรหัสผ่าน
e. การแบ่งแยกสิทธิพิเศษ : ที่เหมาะสม กลไกการป้องกันควรจะต้องการกุญแจสองชั้นในการเปิดออกแทนการใช้กุญแจชั้นเดียว
f. สิทธิพิเศษน้อยที่สุด : โปรแกรมทุกๆ โปรแกรมและผู้ใช้งานทุกคนของระบบ ในการทำงานควรจะใช้สิทธิพิเศษให้น้อยที่สุด
g. กลไกการทำงานร่วมกัน : วิธีการทำงานน้อยที่สุด (หรือการใช้ตัวแปรร่วมกัน) การทำงานร่วมกันมากกว่าหนึ่งคนและต้องพึ่งพาอาศัยกันทุกคน
h. การยอมรับทางด้านจิตใจ : เป็นส่วนประกอบที่สำคัญในการติดต่อกับผู้ใช้ การออกแบบสำหรับการใช้งานต้องสะดวก เช่น ผู้ใช้งานประจำและการประยุกต์ใช้เป็นกลไกการควบคุมโดยอัตโนมัติ

การพัฒนาซอฟต์แวร์ที่มีปัญหาด้านความปลอดภัย (Software Development Security Problems)

ในบางครั้งการพัฒนาซอฟต์แวร์แล้วทำให้เกิดปัญหาในซอฟต์แวร์นั้น เป็นความยุ่งยากหรือเป็นไปไม่ได้ในการนำไปใช้งานในแนวทางของความปลอดภัย มีการค้นพบสิ่งที่เป็นอันตรายในด้านความปลอดภัยของซอฟต์แวร์ มี 19 ปัญหาในการพัฒนาซอฟต์แวร์ (ซึ่งเป็นที่รู้จักดีในสาขาวิศวกรรมซอฟต์แวร์) ที่จัดเป็นหมวดหมู่โดย John Viega ในความต้องการของ Amit Youran ซึ่งเป็นผู้อำนวยการของ Homeland Security's National Cyber Security Division ซึ่งได้แก่

Buffer Overruns

เป็นวิธีการบุกรุกฉวยโอกาสอันเกิดขึ้นจากการที่ไม่มีการตรวจสอบบริเวณหน่วยความจำ ที่เรียกว่าบัฟเฟอร์ของโปรแกรมเพื่อเข้าไปเขียนโค๊ดโปรแกรมและข้อมูลบนหน่วยความจำบริเวณนั้น ถ้าข้อมูลที่เขียนทับเข้าไปเป็นโค๊ดที่สามารถทำงานได้ ก็จะทำให้ขั้นตอนการทำงานของโปรแกรมที่อยู่นั้นเปลี่ยนแปลงได้ตามที่ผู้บุกรุกต้องการ แต่ถ้าคำสั่งที่เขียนเข้าไปเป็นข้อมูลอื่นๆ ผลกระทบที่เกิดขึ้นก็อาจจะทำให้โปรแกรมหยุดทำงาน

Command Injection

เกิดขึ้นเมื่อผู้ใช้ป้อนข้อมูลโดยตรงเข้าไปยังคอมไฟล์เลอร์หรืออินเทอร์พรีเตอร์ ภายใต้ประเด็นความล้มเหลวของผู้พัฒนาไปถึงการรัปประกันคำสั่งที่ป้อนเข้าไปให้ถูกต้องก่อนที่จะใช้โปรแกรม ตัวอย่างง่ายๆ ที่เป็นไปได้เกี่ยวกับคำสั่งของ Windows

@ echo off

set /p myVar="Enter the String"

set somVar=%myVar%

echo %somevar%

นี้เป็นคำสั่งที่ต้องการให้ผู้ใช้ใส่ตัวอักษรง่ายๆ ตัวแปรอื่นๆ แล้วก็แสดงค่าออกมา อย่างไรก็ตามผู้บุกรุกสามารถใช้คำสั่งและตามด้วยตัวอักษร & ให้ต่อกันกับคำสั่งอื่นที่ต้องการ (hello&del*.*)

Cross-site Scripting (XSS)

เกิดชึ้นเมื่อแอพพลิเคชั่นทำงานบนเว็บเซิร์ฟเวอร์รับข้อมูลจากคำสั่งของผู้ใช้เข้ามา ผู้บุกรุกสามารถอาศัยจุดอ่อนของเว็บเซิร์ฟเวอร์ทำการส่งโค๊ด ภาษาที่เว็บบราวเซอร์สามารถเข้าใจ ไปยังหน้าหน้าเว็บที่แสดงโดยเว็บบราวเซอร์ของเหยื่อเพื่อให้เว็บบราวเซอร์ของเหยื่อทำงานตามที่ผู้บุกรุกต้องการ ไม่ว่าจะเป็นการขโมยข้อมูลส่วนบุคคล หรือบังคับให้เว็บบราวเซอร์ทำการโจมตีเป้าหมายที่ผู้บุกรุกต้องการ

Failure to Handle Errors

อะไรจะเกิดขึ้นเมื่อระบบหรือแอพพลิเคชั่นประสบกับเหตุการณ์ที่ไม่ได้เตรียมพร้อมสำหรับการจัดการ มันพยายามทำให้สำเร็จลุล่วง (การอ่าน การเขียนหรือการคำนวณ) ประกาศข่าวสารสำคัญที่ผู้พัฒนาโปรแกรมสามารถเข้าใจ หรือหยุดการทำงาน ความล้มเหลวที่จะจัดการกับข้อผิดพลาดสาเหตุมาจากหลายพฤติกรรมของการใช้ระบบที่ไม่ได้คาดคิดมาก่อน ผู้พัฒนาโปรแกรมที่คาดหมายไว้ล่วงหน้าถึงปัญหาและได้เตรียมพร้อมของโค๊ดแอพพลิเคชั่นที่จะจัดการ

Failure to Protect Network Traffic

ด้วยความเจริญก้าวหน้า ความแพร่หลายของระบบเครือข่ายไร้สายที่เกิดขึ้น สอดคล้องกับการเพิ่มขึ้นในเรื่องความเสี่ยงในการส่งข้อมูลโดยทางเครือข่ายไร้สายจะถูกรบกวน ส่วนใหญ่ระบบเครือข่ายไร้สายจะติดตั้งและทำงานจำนวนน้อยหรือไม่ป้องกัน สารสนเทศนั้นจะกระจายไประหว่าง Client และ Access Point โดยเฉพาะเครื่องขายไร้สายสาธารณะในร้านกาแฟ ร้านหนังสือและโรงแรม โดยปราศจากการเข้ารหัสที่เหมาะสม (เช่น WPA) ผู้บุกรุกสามารถดักจับเพื่อดูข้อมูลได้

การจราจรบนเครือข่ายที่มีสายก็เช่นเดียวกันมีจุดอ่อนในการดักจับบางสถานการณ์บนระบบเครือข่ายที่ใช้ Hub ผู้ใช้งานบางคนสามารถติดตั้งโปรแกรมดักจับหรือข้อมูลในเครือข่าย และรวบรวมการติดต่อสื่อสารจากผู้ใช้บนเครือข่าย บางครั้งจะ Scan โดยไม่ได้รับอนุญาตในการจับ Packet บนเครือข่าย ไม่ได้รับอนุญาตให้เชื่อมต่อในระบบเครือข่าย และโดยทั่วไปการตระหนักถึงการคุกคามสามารถทำให้ปัญหาลดลง

Failure to Store and Protect Data Securely

การเก็บรักษาและป้องกันข้อมูลอย่างปลอดภัยเป็นประเด็นใหญ่มาก ผู้พัฒนาโปรแกรมเป็นผู้รับผิดชอบในการควบคุมการเข้าถึง และการเก็บรักษาความปลอดภัยของสารสนเทศออกจากโปรแกรม การควบคุมการเข้าเป็นประเด็นของการควบคุมดูแลว่า ใครทำอะไร เมื่อไหร่ ที่ไหน อย่างไร และมีผลกับข้อมูลระบบ ความล้มเหลวในการจัดเตรียมเครื่องมือหรือวิธีการอย่างเหมาะสม การควบคุมการเข้าถึงที่อ่อนแอทำให้ข้อมูลไร้ความมั่นคง การเคร่งครัดควบคุมการเข้าถึงเป็นอุปสรรคของการใช้งานทางธุรกิจ เป็นอุปสรรคในเรื่องสมรรถนะและประสิทธิภาพของเครื่องและมีความเสี่ยงในการดำเนินการควบคุม การโอนย้ายหรือในทางอ้อม

การรวมเข้าด้วยกันของความปลอดภัยสารสนเทศ เช่น การฝังข้อมูลรหัสผ่านลงในโค๊ด ทำการเข้ารหัสหรือสารสนเทศที่ไวต่อความรู้สึกของผู้อื่น เป็นการเสี่ยงต่อการถูกเปิดเผย

Failure to Use Cryptographically Strong Random Numbers

ระบบการเข้ารหัสส่วนมากจะทันสมัยเหมือนกับระบบคอมพิวเตอร์อื่นๆ ใช้การสุ่มหมายเลขที่สร้างขึ้น อย่างไรก็ตามระบบการตัดสินใจในการสุ่มและเลขสุ่มเทียมสำหรับวิธีการ Monte-Carlo ในการคำนวณล่วงหน้าไม่ต้องการเช่นลำดับขั้น สำหรับความเข้มงวดต้องการความถูกต้องไม่มีแบบแผนดังที่ระบบนั้นการตรวจสอบ เครื่องมือ กระบวนการเข้ารหัสเหล่านี้สุ่มหมายเลขที่สร้างขึ้นโดยใช้ขั้นตอนวิธีทางคณิตศาสตร์ บนพื้นฐานของค่าที่ได้รับเลือกและส่วนประกอบอื่นๆ อีก (เช่นนาฬิกาคอมพิวเตอร์) เพื่อจำลองแบบการสุ่มตัวเลข เหล่านั้นผู้ที่เข้าใจวิธีการทำงานของการสุ่มตัวเลขสามารถคาดเดาได้

Format String Problems

ภาษาคอมพิวเตอร์มีความยืดหยุ่น มีส่วนประกอบพร้อมสำหรับการสร้างความสามารถในการเปลี่ยนแปลงรูปแบบตลอดเวลาที่ต้องการผลลัพธ์ รูปแบบโครงสร้างเป็นทางการคือ รูปแบบที่ใช้กำหนดลักษณะการรับข้อมูล เป็นสิ่งที่หลีกเลี่ยงยากบางครั้งในการพัฒนาโปรแกรมอาจจะใช้ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ เช่น รูปแบบที่ใช้กำหนดลักษณะการรับข้อมูล(เช่น %x, %d, %p) ผู้บุกรุกจะฝังคำสั่งซึ่งมีความหมายตามรูปแบบที่มีจุดประสงค์ร้ายป้อนเข้าไป และโปรแกรมจะแปลความหมายข้อมูลที่ป้อนเข้าไปตามรูปแบบที่สั่ง (เช่น การใช้งานฟังก์ชั่น printf ในภาษา C ให้โปรแกรมแสดงผลออกมา ผู้บุกรุกก็จะสามารถเข้าถึงสารสนเทศหรือเขียนเป้าหมายส่วนที่ต้องการของโปรแกรมซ้อนทับเข้าไปด้วยข้อมูลที่เลือก

Neglecting Change Control

ผู้พัฒนาใช้กระบวนการที่มีชื่อเสียง เช่น การควบคุมการเปลี่ยนแปลงในการทำให้แน่ใจว่าระบบส่งมอบถึงผู้ใช้ แสดงให้เห็นจุดหมายของผู้พัฒนาตอนเริ่มขั้นตอนการพัฒนา การควบคุมการเปลี่ยนแปลงให้แน่ใจว่าผู้พัฒนาไม่ทำงานคนละทาง โดยการแก้ไขบางโปรแกรมหรือส่วนหนึ่งของโปรแกรมในช่วงเวลาใดเวลาหนึ่ง ระบบในกระบวนการผลิต กระบวนการควบคุมการเปลี่ยนแปลงทำให้แน่ใจ แต่การอนุญาตเปลี่ยนแปลง การแนะนำให้รู้จัก และการเปลี่ยนแปลงทั้งหมดนั้นการทดสอบอย่างเพียงพอก่อนที่จะออกเป็นรุ่นปัจจุบัน

Improper File Access

ถ้าผู้บุกรุกเปลี่ยนที่เก็บไฟล์ โดยการขัดขวางและแก้ไขโค๊ดของโปรแกรม พวกเขาสามารถบังคับโปรแกรมในการใช้สิทธิ์เจ้าของไฟล์ แทนที่ไฟล์โปรแกรมซึ่งทึกทักว่าเป็นจริงเพื่อใช้งาน รูปแบบการบุกรุกมีโอกาสใช้อย่างใดอย่างหนึ่ง ปลอมแปลงแทนที่ไฟล์เพื่อให้ไฟล์นั้นมีผลตามกฎหมาย (เช่น ไฟล์รหัสผ่าน) หรือลวงให้ระบบทำงานให้สำเร็จ ความเป็นไปได้สำหรับความเสียหายหรือสิ่งที่ถูกเปิดเผยรุนแรงเกินไป ดังนั้นสิ่งที่เป็นอันตรายที่จะป้องกันไม่ใช่เฉพาะตำแหน่งที่อยู่ของไฟล์ แต่ควรจะเป็นวิธีการและช่องทางการติดต่อสื่อสารโดยสิ่งที่เข้าถึงไฟล์เหล่านั้น

Improper Use of SSL

ผู้พัฒนาโปรแกรมใช้ระบบรักษาความปลอดภัยของข้อมูล (SSL) ในการที่จะส่งข้อมูลที่ละเอียดอ่อนรวมถึงหมายเลขบัตรเครดิตและข้อมูลส่วนบุคคลอื่นๆ ระหว่าง Client และ Server ขณะที่ผู้พัฒนาโปรแกรมส่วนมากนั้นคิดว่าการใช้ระบบรักษาความปลอดภัยของข้อมูล รับประกันความปลอดภัยแต่ไม่ประสบความสำเร็จ มากกว่าการทำให้ประสบความสำเร็จของเทคโนโลยี SSL (Secure Socket Layer) และ TLS (Transport Layer Security) ทั้งสองต้องการพิสูจน์ทำให้ถูกต้องที่ปลอดภัยจริงๆ ความล้มเหลวในการใช้ความปลอดภัย HTTP เพื่อชอบด้วยกฎหมายด้วยใบรับรองอิเล็กทรอนิกส์ และต่อใบรับรองให้ถูกต้องหรือความถูกต้องของสารสนเทศเปรียบเทียบกับรายการของการเพิกถอนใบรับรอง สามารถยอมรับความปลอดภัยของการสื่อสาร SSL

Information Leakage

มีจำนวนมากที่เป็นแนวทางร่วมกันในการจำแนกสารสนเทศโดยตรงและโดยอ้อม สมัยสงครามโลกครั้งที่ 2 ทหารประกาศเตือนใช้คำว่า “ปากหลวม เรือล่ม” ให้ความสำคัญกับความเสี่ยงการเคลื่อนพลทางเรือ จากฝ่ายตรงข้ามจะกระทำกับลูกเรือ เรือเดินทะเล และการเปิดเผยจากภายในของการเคลื่อนไหวของเรือ คือการแบ่งปันอย่างกว้าง ความกลัว อันตรายที่พลเรือนได้รับ คอยปฏิบัติงานในสิ่งกีดขวางและที่ทำงานร่วมพอร์ตของกองทัพเรือ ขณะที่กำลังคอยสิ่งที่จะลงมา โดยการเตือนลูกจ้างเกี่ยวกับการเปิดเผยสารสนเทศ องค์กรสามารถป้องกันความปลอดภัยของการดำเนินการ

Integer Bugs (Overflows/Underflows)

แม้ว่าสมุดและดินสอสามารถรับมือเกี่ยวกับจำนวนของตัวเลข เลขฐานสองถูกใช้ในคอมพิวเตอร์โดยการกำหนดความยาวโดยเฉพาะ เช่น จำนวน 1 ถึง 32,767 จะได้จำนวน 32,768 แต่ในระบบตัวเลขด้วยเครื่องหมายจำนวนเต็ม 16 บิท ผลลัพธ์คือ -32,768 จำนวนน้อยมากจนไม่สามารถนำเก็บในหน่วยความจำได้สามารถเกิดขึ้นเมื่อ เช่น ลบออก 5 จาก -32,767 ให้ผลลัพธ์อย่างแปลกใจด้วย +32,764 เพราะว่าจำนวนเต็มที่เป็นลบมากมายสามารถแสดงใน 16 บิทที่เป็นลบคือ -32,768

ข้อผิดพลาดของจำนวนเต็มนี้เกิดขึ้นด้วยกัน 4 ประเภทคือ

1. ล้นมากเกินไปหมายถึงหน่วยความจำไม่สามารถรับข้อมูลเข้าไปได้อีก
2. น้อยมากเกินไปจนไม่สามารถเก็บในหน่วยความจำได้
3. การตัดจำนวนบิทส่วนเกินทิ้งไปในการจัดเก็บจำนวนจริง

4. ข้อผิดพลาดที่เกิดจากการยอมจำนน ความผิดพลาดของจำนวนเต็มโดยปกติเป็นการกระทำโดยทางอ้อม

กลไกความผิดพลาดของจำนวนเต็มเปิดโอกาสให้ผู้บุกรุกเข้าไปใช้พื้นที่อื่นๆ ของหน่วยความจำ แอพพลิเคชั่นโดยควบคุม หน่วยความจำจัดสรรค่าที่ได้รับมามากกว่า ถ้าค่านั้นดีกว่าที่คาดไม่ถึงด้วยบิทพิเศษเขียนเข้าไปในสถานที่อื่นๆ ระบบอาจจะมีประสบการณ์ผลลัพธ์ที่ไม่คาดคิด อันทำให้สามาถคำนวนผิด การกระทำผิด เกิดการล้มละลายหรือมีปัญหาอื่นๆ “แม้ว่าความผิดพลาดของจำนวนเต็มเป็นประจำ ทำให้เกิดการเขียนข้อมูลเกินขอบเขตที่กำหนด หรือหน่วยความจำอื่นๆ ถูกยึด ความผิดพลาดของจำนวนเต็มไม่ใช่กรณีพิเศษของหน่วยความจำทำงานผิดพลาด”

Race Conditions

คือความล้มเหลวของโปรแกรมเกิดขึ้นอย่างฉับพลัน ในการสั่งงานพร้อมกันในการดำเนินการของโปรแกรม ผลของความขัดแย้งตลอดการเข้าไปใช้ทรัพยากรของระบบร่วมกัน การขัดแย้งไม่ต้องการเกี่ยวกับสตรีมของโค๊ดภายในโปรแกรมเนื่องจากระบบปฏิบัติการและเทคโนโลยีโปรเซสเซอร์แยกการทำงานโดยอัตโนมัติในหลายเส้นทางนั้น สามารถดำเนินการในเวลาเดียวกันถ้าบนเส้นทางของผลลัพธ์จากการแชร์โปรเซส ทรัพยากรอื่นๆ เหล่านั้นสามารถจะติดต่อกับผู้ใช้ซึ่งกันและกัน

การเกิด Race Conditions เช่น โปรแกรมสร้าง Temporary ไฟล์ และผู้บุกรุกสามารถทำการทำซ้ำในระหว่างเวลาที่สร้างและเวลาที่ใช้ Race Conditions สามารถเกิดขึ้นเช่นเดียวกันพร้อมกับการเก็บสารสนเทศในหน่วยความจำหลายเส้นทาง ถ้าหนึ่งเส้นทางเก็บสารสนเทศในตำแหน่งหนวยความจำผิดโดยบังเอิญหรือเจตนา

SQL Injection

เกิดขึ้นเมื่อผู้พัฒนาระบบประสบความล้มเหลว ในการใส่ข้อมูลผู้ใช้เข้าไปก่อนการใช้ Query ฐานข้อมูล เช่น โดยความจริงโปรแกรมที่ไม่เป็นอันตรายส่วนรับ User ข้อมูลเข้า User-ID และหลังจากการทำคำสั่ง SQL Query เปรียบเทียบตาราง User ที่ได้รับ ตัวอย่างเช่น

```
Accept USER-ID from console;
SELECT USER-ID, NAME FROM USERS WHERE USERID = USER-ID;
```

นี้เป็นรูปแบบ SQL โดยเฉพาะและเมื่อใช้คำสั่งถูกต้องจะแสดง USERID และชื่อผู้ใช้ปัญหาคือข้อมูลที่ได้รับจะผ่านโดยตรงไปยัง SQL Database Server และส่วนของคำสั่ง SQL และถ้าผู้บุกรุกป้อนตัวอักษร “JOE or 1=1” ตัวอักษรนี้ร่วมกับบ้างส่วนมีผลต่อรูปแบบ SQL จะตอบกลับแถวทั้งหมดจากตารางที่ USER-ID เหมือนกันคือ “JOE or 1=1” เพราะว่า 1 เท่ากับ 1 ผลลัพธ์ทั้งหมดคือ USER-ID และ Name จะตอบกับ สิ่งที่เป็นไปได้ทำให้เกิดความสามารถที่ “Inject” SQL ของผู้บุกรุกเลือกใส่เข้าไปในโปรแกรมไม่ต้องมีขอบเขตที่เหมาะสมเข้าถึงสารสนเทศ ถ้าผู้บุกรุกใช้คำสั่ง SQL ลบตารางผู้ใช้หรือทำการปิดระบบฐานข้อมูล

Trusting Network Address Resolution

Domain Name Service (DNS) เป็นการทำงาน WWW ในการแปลง URL (Uniform Resource Locator) เช่น http://www.course.com เป็น IP Address ของเว็บเซิร์ฟเวอร์ รูปแบบการ

เผยแพร่นี้ถูกโจมตีได้ง่ายหรือเป็นอันตราย DNS แคชเป็นอันตรายที่เกี่ยวข้องกับการยอมรับ เวลาเปลี่ยนแปลง DNS Server ต้องการ IP Address สัมพันธ์กันกับ Domain Name เป็นวิธีหนึ่งที่ผู้บุกรุกเลือกใช้การปลอมแปลง การออกแบบเว็บไซต์ที่ผลิตจากสารสนเทศส่วนบุคล หรือสิ่งนั้นมีประโยชน์มากสำหรับผู้บุกรุก เช่นการเปลี่ยนเว็บไซต์ร้านค้าคู่แข่ง เป็นมากกว่าการมุ่งร้าย เช่น การปลอมแปลงเว็บไวต์ Banking สำหรับ Phishing Attack เกี่ยวกับสารสนเทศ Banking ออนไลน์

วิธีการหนึ่งในการปลอมแปลงข้อมูลสารสนเทศใน DNS Server ส่วนมากพยายามสร้างเกี่ยวกับ DNS Server หลักและสำรองขององค์กร ความพยายามโจมตีอื่นๆ ที่เป็นอันตราย DNS Server มาขึ้นทวีคูณ ระบบ DNS อาศัยกระบวนการปรับปรุงอัตโนมัติที่สามารถประสบความสำเร็จ ผู้บุกรุกส่วนมากโดยปกติเป็นอันตรายในส่วนของ DNS อย่างใดอย่างหนึ่งโดยการโจมตี Name Server และการแทนที่ของ DNS หลักโดยการปรับปรุงข้อมูลส่วนบุคคลไม่ถูกต้องหรือโดยการตอบสนองก่อน DNS จริงจะทำ ชนิดท้ายสุดของการบุกรุก ถ้าผู้บุกรุกค้นพบความล้าช้าใน Name Server เขาสามารถติดตั้งเครื่องอื่นให้ตอบสนอง ทั้งที่ DNS จริงยังคงอยู่ ก่อน DNS Server จริงจะตอบสนอง Client ได้รับครั้งแรกของชุดสารสนเทศที่ได้รับและโดยตรงถึง IP Address

Unauthenticated Key Exchange

หนึ่งของความยิ่งใหญ่อันท้าทายในระบบ Private key ซึ่งเกี่ยวกับผู้ใช้สองคนใช้งานร่วมกุญแจเดียวกัน คือต้องการเพื่อได้กุญแจกับกลุ่มอื่นอย่างปลอดภัย บางครั้งจะนอกสัญญาณ ผู้ส่งข่าวเป็นผู้ถูกใช้ในเวลาอื่นระบบ Public key ซึ่งใช้ทั้งสอง Public และ Private key เป็นการใช้แลกเปลี่ยนกุญแจแต่สิ่งที่ถ้าบุคคลซึ่งได้รับสถานที่กุญแจบนอุปกรณ์ USB และการส่งไม่แท้จริงงานของบริษัทแต่ความคาดหวังอย่างง่ายโดยเฉพาะการส่งมอบและการขัดขวาง เรื่องเดียวกันนี้เกิดขึ้นบนอินเทอร์เน็ต เมื่อผู้บุกรุกเขียนแก้ไขระบบ Public key และแทนที่ออกในขณะที่ฟรีแวร์ การทำให้เสื่อมหรือการขัดขวางการทำงานของบางคน อื่นอีกของระบบการเข้ารหัส Public key อาจเป็นไปได้โดยตัวแทนที่ได้เตรียม Public key

Use of Magic URLs And Hidden Forms

HTTP เป็นโปรโตคอลที่ไม่มีการรู้จำสถานะที่โปรแกรมคอมพิวเตอร์อันใดอันหนึ่ง สุดท้ายช่องทางของการติดต่อสื่อสารไม่สามารถไว้วางใจที่รับประกันการส่งข่าวสาร สิ่งนั้นให้ยุ่งยากสำหรับการพัฒนาที่ระบุการเปลี่ยนของผู้ใช้ด้วยเว็บไซต์หลายอันตลอดการปฏิสัมพันธ์ เป็นประจำด้วยการตอบสนองต่อสภาพสารสนเทศเป็นอย่างง่ายรวมอยู่ในอย่างน่าอัศจรรย์ของ URL (Authentication ID ที่ใช้ในการผ่านค่าตัวแปรใน URL สำหรับการแลกเปลี่ยนการดำเนินงานตามต้องการ)หรือรวมอยู่ในการซ่อนรูปแบบฟิลค์บนหน้าเว็บเพจ ถ้าสารสนเทศนั้นเป็นเก็บข้อมูลที่อยู่ในรูปแบบที่อ่านได้ ผู้บุกรุกสามารถเก็บเอาสารสนเทศจากความน่าอัศจรรย์ของ URL ในขณะที่ท่องไปในเครือข่ายหรือใช้สคริพท์บนเครื่องผู้ใช้แก้ไขข้อมูลที่ซ่อนอยู่ในรูปแบบฟิลค์ ขึ้นอยู่กับโครงสร้างของแอพพลิเคชั่น, การเก็บ/การแก้ไขสารสนเทศ สามารถจะใช้ในการลวง/การบังคับหรือการเปลี่ยนการทำงานทางแอพพลิเคชั่น (เช่น รายการของราคาเก็บซ่อนอยู่ในรูปแบบฟิลด์ ผู้บุกรุกสามารถแก้ไขราคาเพื่อซื้อสินค้าชิ้นนั้น)

Use of Weak Password-Base Systems

ความล้มเหลวที่ต้องการเพียงรหัสผ่านที่เข็มแข็ง และการควบคุมรหัสผ่านที่ใช้ไม่เหมาะสม คือประเด็นความปลอดภัยอื่นๆ ที่รุนแรง นโยบายรหัสผ่านสามารถกำหนดตัวเลขและชนิดของตัวอักษร ความถี่ของการบังคับให้เปลี่ยนและแม้แต่การนำรหัสผ่านเก่ากลับมาใช้ เช่นเดียวกับผู้ดูแลระบบสามารถควบคุมตัวเลขที่นำมาใช้ไม่เหมาะสม นั้นคือการทำโดยผู้ใช้และปรับปรุงมากขึ้นขยายระดับของการป้องกัน ระบบนั้นไม่ทำรหัสผ่านให้ถูกต้องหรือการเก็บรหัสผ่านในสถานที่เข้าถึงได้ง่ายสำหรับผู้บุกรุก ความแข็งแรงของรหัสผ่านมีผลโดยตรงกับความสามารถที่จะทนต่อการถอดรหัส การใช้ไม่เป็นมาตรฐานในส่วนประกอบของรหัสผ่าน ต้องไม่น้อยกว่า 8 ตัวอักษรด้วยอย่างน้อยต้องมีหนึ่งตัวพิมพ์ใหญ่ ตัวเลข และตัวอักษรที่ไม่ใช่ตัวเลข สามารถทำให้ความแข็งแรงของรหัสผ่านมากขึ้น

ตารางแสดงสมรรถภาพของรหัสผ่าน

Case-Insensitive Password

จำนวนของตัวอักษร	โอกาสที่จะเป็นไปได้ของการถอดรหัส	เวลาที่ใช้ในการถอดรหัส
1	68	0.000009 second
2	4,624	0.006 second
3	314,432	0.04 second
4	21,381,376	2.7 seconds
5	1,453,933,568	3 minutes, 2 seconds
6	98,867,482,624	3 hours, 26 minutes
7	6,722,988,818,432	9 days, 17 hours, 26 minutes
8	457,163,239,653,376	1 years, 10 months, 1 day
9	31,087,100,296,429,600	124 years, 11 months, 5 days
10	2,113,922,820,157,210,000	8495 years, 4 months, 17 days

Case-Sensitive Password

จำนวนของตัวอักษร	โอกาสที่จะเป็นไปได้ของการถอดรหัส	เวลาที่ใช้ในการถอดรหัส
1	94	0.00001 second
2	8,836	0.011 second
3	830,584	0.1 second
4	78,074,896	9.8 seconds
5	7,339,040,224	15 minutes, 17 seconds
6	689,869,781,056	23 hours, 57 minutes 14 seconds
7	64,847,759,419,264	3 months, 3 days, 19 hours
8	6,095,689,385,410,820	24 years, 6 months
9	572,994,802,228,617,000	2302 years, 8 months, 9 days
10	53,861,511,409,000,000	216,457 years, 4 months

Poor Usability

บุคคลชอบการกระทำในสิ่งที่ง่าย เมื่อต้องพบกับการปฏิบัติงานที่เป็นทางการ และแบบไม่เป็นทางการเป็นสิ่งที่ง่ายเขาทั้งหลายชอบวิธีการที่ง่าย วิธีที่ดีที่อ้างอิงตำแหน่งที่เป็นประเด็นคือเตรียมให้เพียงแค่ทางเดียว ทางที่ปลอดภัยการผสมผสานความปลอดภัย ความสามารถ เพิ่มการอบรม ความตระหนักและทำให้แน่ใจเสถียรภาพของการควบคุมทั้งหมด รับผิดชอบต่อความปลอดภัยของสารสนเทศ อนุญาตให้ผู้ใช้ใช้ค่ามาตรฐานเพื่อให้ง่าย วิธีการใช้สะดวกมากกว่า ซึ่งหลีกเลี่ยงที่จะนำมาสู่ความเสียหาย

สรุป

- ความปลอดภัยของข้อมูลมีหน้าที่สำคัญ 4 อย่างคือ
  - การป้องกันการทำงานของระบบต่างๆในองค์กร
  - ปกป้องการดำเนินงานของโปรแกรมให้ปลอดภัย
  - การป้องกันข้อมูลที่องค์กรใช้และเก็บรวบรวม
  - ปกป้องทรัพย์สินเทคโนโลยีในองค์กร
- การจัดการเกี่ยวกับความปลอดภัยของข้อมูล ต้องรู้ว่าภัยคุกคามนั้นมีผลกระทบกับคน โปรแกรม ข้อมูลและระบบสารสนเทศอย่างไร
- ภัยคุกคามหรืออันตรายที่กระทบกับพนักงาน ข้อมูล และระบบขององค์กร แบ่งได้ 12 ประเภท
  - ข้อผิดพลาดจากการกระทำของมนุษย์
  - การละเมิดทรัพย์สินทางปัญญา
  - การบุกรุก
  - การกรรโชกข้อมูลสารสนเทศ
  - การก่อวินาศกรรมหรือการทำลาย
  - การโจรกรรม
  - การโจมตีซอฟต์แวร์
  - ภัยธรรมชาติ
  - คุณภาพของบริการ
  - ความล้มเหลวหรือข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์
  - ความล้มเหลวหรือข้อผิดพลาดทางเทคนิคของซอฟต์แวร์
  - เทคโนโลยีล้าสมัย
- การโจมตีที่ได้ผล คือทำกับระบบที่มีไม่มั่นคง ถ้าสามารถโจมตีได้สำเร็จจะทำความเสียหาย หรือขโมยข้อมูลสารสนเทศ หรือ ทรัพย์สินขององค์กรได้ องค์กรต้องค้นหาจุดอ่อนของระบบควบคุมสิ่งใดบ้างที่หน่วยควบคุมไม่แสดงผล หรือ ไม่มีประสิทธิภาพ

- การประกันซอฟต์แวร์ (SA) กำหนดระเบียบเกี่ยวกับความปลอดภัยของคอมพิวเตอร์ และกำหนดกิจกรรมที่มีส่วนในการสร้างระบบที่มีความปลอดภัย

- ขั้นตอนการพัฒนาซอฟต์แวร์ที่ไม่ดี มีส่วนสำคัญต่อการเกิดความเสี่ยง แต่ด้วยการพัฒนาที่ดีนั้นมีหลักปฏิบัติดังนี้ การเปลี่ยนตัวควบคุม และการประกันคุณภาพของกระบวนการ เป็นการประกันคุณภาพซอฟต์แวร์ทั้งหมด เพื่อประสิทธิภาพความปลอดภัยของซอฟต์แวร์ที่เพิ่มขึ้นต่อเนื่อง

****

บรรณานุกรม

Whitman, M. E & Mattord, H. J. **Principles of Information Security**. (3rd ed.). USA:Course Technology.

Anderson, James P. 1980. "Computer Security Threat Monitoring and Surveillance". James P. Anderson Co., Fort Washington, Pennsylvania

Bace, Rebecca and Mell, Peter. (2001). “Intrusion Detection Systems(IDS)”. NIST Computer Security Special Publication. (online). http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

Price, Katherine. 1998. “Characteristics of a Good Intrusion Detection System” COAST. (online). http://www.cerias.purdue.edu/about/history/coast_resources/idcontent/detection.html

SANS Institute. (2001). “NSA Glossary of Terms Used in Security and Intrusion Detection”. (online). http://www.sans.org/newlook/resources/glossary.htm

Supachoke Sukkasame. (2005). “การวิเคราะห์ข้อมูลกิจกรรมของระบบเพื่อตรวจจับการบุกรุก”. A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science Prince of Songkla University

ThaiCERT. (2001). “ระบบตรวจจับการบุกรุก (Intrusion Detection System)”. (online).
http://www.thaicert.org/paper/ids/ids.php
http://www.movestation.org/forum/viewthread.php?tid=726
http://pclab.nectec.or.th/Documents/Support/Article/Malware.pdf
http://elearning.su.ac.th/~elearn/Doc/Malware.pdf
http://www.issp.co.th/2006/article_01.html
http://support.activemedia.co.th/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=27
http://www.acisonline.net/article_prinya_malware.htm A.Pinya Hom-anek, GCFW, CISSP, CISA ACIS Professional Team บัญญัติ 10 ประการ สำหรับการปราบ Malware ต่างๆ ในองค์กร