บทที่ 7 ภัยคุกคามความมั่นคงระบบสารสนเทศ

คำนำ

ปัจจุบันอินเตอร์เน็ตมีความสำคัญต่อการดำเนินกิจกรรมต่างๆ ทั้งการใช้งานส่วนตัว การดำเนินงานทั้งภาครัฐและเอกชน โดยเฉพาะอย่างยิ่งองค์กรที่ต้องการเชื่อมต่อเครือข่ายภายในกับเครือข่ายภายนอก เพื่อที่จะได้รับประโยชน์จากการทำธุรกรรมต่างๆ ย่อมมีความเสี่ยงจากภัยคุกคาม

ดังนั้นองค์กรควรให้ความสำคัญกับการป้องกันความปลอดภัยของข้อมูล และระบบสารสนเทศให้มั่นคงปลอดภัยจากการโจมตีระบบ ซึ่งพนักงานทุกคนต้องตระหนึกถึงความสำคัญ และร่วมมือปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูล จึงจะเกิดระบบที่มีประสิทธิภาพ

การบริหารจัดการความมั่นคงระบบสารสนเทศ“The Need for Security”

บทนำ

นโยบายและกลยุทธ์ด้านเทคโนโลยีสารสนเทศหลายๆ นโยบายและกลยุทธ์นั้นมีความแตกต่างกัน หน้าที่หลักของนโยบายและกลยุทธ์ป้องกันภัยข้อมูลสารสนเทศ เป็นสิ่งที่ทำให้แน่ใจว่าระบบสารสนเทศยังคงอยู่เหมือนเดิม โดยที่องค์กรนั้นจ่ายเงินเป็นหลักร้อย หลักพันดอลล่าร์ สำหรับชั่วโมงการทำงานของพนักงานที่ทำหน้าที่ดูแลรักษาระบบสารสนเทศ ถ้าการคุกคามข้อมูลสารสนเทศและระบบยังไม่หมดไป องค์กรควรปรับปรุงระบบอย่างสม่ำเสมอ เพื่อสนับสนุนข้อมูลสารสนเทศอย่างไรก็ตามการโจมตีระบบข้อมูลสารสนเทศเป็นเหตุการณ์ที่เกิดขึ้นเป็นประจำทุกวัน และต้องการการรักษาความปลอดภัยของข้อมูลสารสนเทศที่เพิ่มมากขึ้น พร้อมกับการโจมตีที่มีความซับซ้อนมากขึ้นองค์กรต้องเข้าใจในสิ่งแวดล้อมของการทำงานของระบบข้อมูลสารสนเทศ ดังนั้นนโยบายและกลยุทธ์ป้องกันภัยข้อมูลสารสนเทศจึงจะสามารถจัดการปัญหาต่างๆ ได้ จะเห็นได้ว่าในบทนี้จะพูดถึงเรื่องสภาพแวดล้อมและการระบุถึงภัยคุกคาม ซึ่งเป็นต้นเหตุที่เกิดขึ้นกับข้อมูลสารสนเทศในองค์กร

สิ่งที่องค์กรต้องการ (Organization Need First)

การรักษาความปลอดภัยของข้อมูลสารสนเทศ มีส่วนประกอบสำคัญ 4 ส่วนได้แก่

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

การป้องกันการทำงานของระบบต่างๆในองค์กร (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 Woodกล่าวว่า"ในความเป็นจริงความปลอดภัยของข้อมูลเกิดจากการจัดการทางเทคโนโลยีสารสนเทศที่ดีผู้คนจำนวนมากคิดที่จะแก้ไขเทคโนโลยี มากกว่าการแก้ปัญหาของเทคโนโลยี คิดเพียงว่า เป็นการดีไม่ต้องมาเพิ่มงานฉันให้มากขึ้น 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 เพราะฉะนั้นจะต้องให้ความสำคัญกับการปกป้องข้อมูลที่มีการเคลื่อนไหวและข้อมูลที่เหลือให้ได้รับความปลอดภัย ไม่ให้ข้อมูลถูกแฮกเกอร์ขโมย หรือ ทำการแก้ไขข้อมูล ระบบรักษาความปลอดภัยที่มีประสิทธิภาพต้องมีการวางแผนการป้องกัน เพื่อให้ข้อมูลขององค์กรมีความถูกต้องครบถ้วน ไม่ถูกแก้ไข

ปกป้องทรัพย์สินเทคโนโลยีในองค์กร (Safeguarding Technology Assets inOrganization)

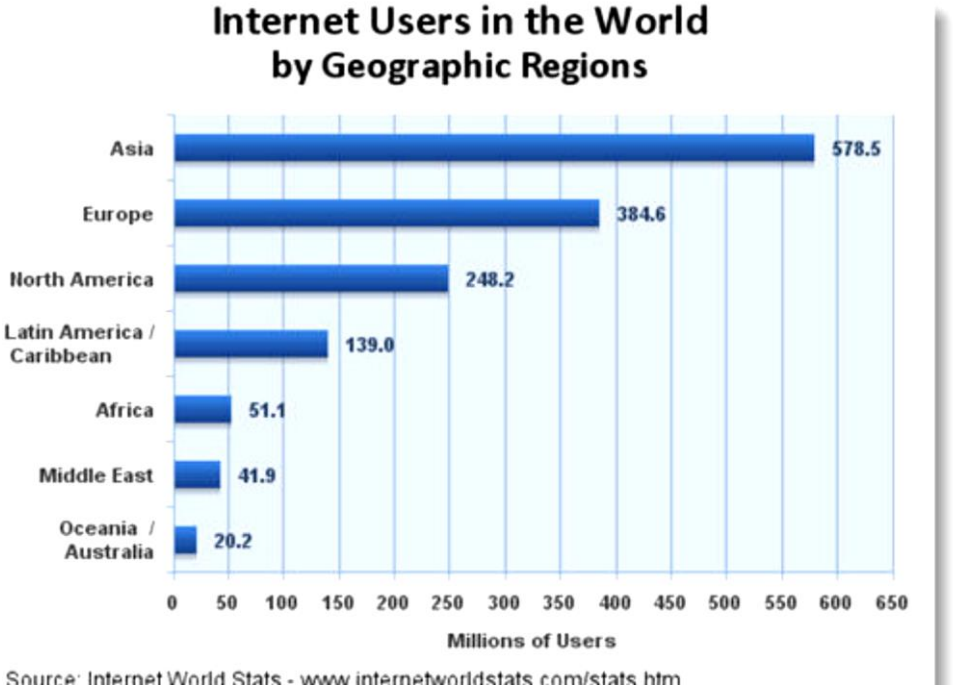
แม้องค์กรจะมีการปฏิบัติงานที่มีประสิทธิภาพ ยังคงต้องการเพิ่มบริการโครงสร้างพื้นฐานที่มีความปลอดภัยตามขนาดและขอบเขตขององค์กร เช่น ธุรกิจขนาดเล็กอาจจะมีผู้ให้บริการอินเตอร์เน็ตเป็นผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ และเครื่องมือในการสร้างรหัสส่วนบุคคล เมื่อองค์กรเติบโตจะต้องพัฒนาการบริการความปลอดภัยเพิ่มขึ้นด้วยเช่นกัน ยกตัวอย่าง การที่องค์กรขยายตัวเพิ่มขึ้นมีการทำธุรกรรมอิเล็กทรอนิกส์ ต้องทำให้ระบบได้รับความเชื่อถือ และมีความปลอดภัยในการติดต่อกับบุคคลและองค์กรภายนอก จะต้องมีเทคโนโลยีความปลอดภัยมาช่วยก็คือ Public KeyInfrastructure (PKI) เป็นการรวมกันของซอฟต์แวร์ระบบต่างๆ เช่น การสร้างรหัสลับ และ ข้อตกลงทางกฎหมายเพื่อสนับสนุนโครงสร้างพื้นฐานข้อมูลทั้งหมดขององค์กร รวมถึงใบรับรองอิเล็กทรอนิกส์ลายมือชื่ออิเล็กทรอนิกส์ทำให้แน่ใจว่าการติดต่อธุรกิจผ่านทางอินเตอร์เน็ตเป็นความลับ ใบรับรองอิเล็กทรอนิกส์เป็นชุดข้อมูลอิเล็กทรอนิกส์มีข้อความและตัวเลขแสดงและระบุการมีตัวตนของผู้ถือใบรับรอง ทำให้แน่ใจว่าระบบสารสนเทศของผู้ให้บริการมีใบรับรอบอิเล็กทรอนิกส์ ข้อมูลต่างๆมีการตรวจสอบความถูกต้อง และผู้ใช้บริการจะได้ข้อมูลที่ถูกต้อง ครบถ้วนถ้าเครือข่ายขององค์กรมีการขยายตัว 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 รู้จักการปกป้องข้อมูลและระบบให้มีความมั่น คง ระบบขนส่ง และขั้นตอนต่างๆ

2) การรู้ถึงภัยคุกคามที่ต้องเผชิญ ศึกษาจากแหล่งข้อมูลที่น่าเชื่อถือทำให้สามารถตัดสินใจจัดการกับภัยคุกคามต่างๆที่มีผลกับ พนักงาน โปรแกรม ข้อมูล และระบบสารสนเทศขององค์กร การรักษาความปลอดภัยข้อมูล กล่าวถึงอันตรายจากภัยคุกคามที่ส่งผลกับคน และทรัพย์สินมีการสำรวจประเภทของภัยคุกคาม เมื่อการเชื่อมต่ออินเตอร์เน็ตขยายไปทั่ว โลก ศึกษาถึงแนวทางปฏิบัติในการป้องกันภัยคุกคามต่างๆ มีการสำรวจเปรียบเทียบประเภทของภัยคุกคามทำให้เกิดความเข้าใจร่วมกันว่าภัยคุกคามที่เพิ่มขึ้นมาจากการที่องค์กรเชื่อมต่ออินเตอร์เน็ต โดยจำนวนผู้ใช้อินเตอร์เน็ตเพิ่มขึ้นเรื่อยๆ คิดเป็น 17% ของคนทั้งโลก หรือ จากคนทั่ว โลก 6.6 พันล้านคน มีคนที่เข้าใช้งานอินเตอร์เน็ตถึง 1.1 พันล้านคน



รูปแสดงการใช้อินเตอร์เน็ตทั่ว โลก

ปี 2006 Computer Security Institute (CSI) ซึ่งเป็นหน่วยงานของ FBI ทำการสำรวจอาชญากรรมคอมพิวเตอร์และการรักษาความปลอดภัย จากการศึกษาพบว่า 72% ที่ตอบสนอง(บริษัทขนาดใหญ่และหน่วยงานราชการ) ตรวจพบการฝ่าฝืนการรักษาความปลอดภัยทางอินเตอร์เน็ตภายใน 12 เดือนล่าสุด อีก 52% เข้าใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งลดลงจาก56% ในปี 2005ตารางต่อไป 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 สิ่งเล็กน้อยเหล่านี้สามารถสร้างความเสียหายอย่างมากการคุกคามที่อันตรายที่สุดต่อความปลอดภัยของข้อมูลองค์กร คือ พนักงานขององค์กรเองเพราะพนักงานใช้ข้อมูลในการดำเนินกิจกรรมทางธุรกิจขององค์กรทุกวัน สิ่งที่พนักงานจะต้องปฏิบัติอย่างเคร่งครัดคือ การรักษาความลับของข้อมูล ข้อมูลมีความถูกต้องครบถ้วน และข้อมูลพร้อมใช้งานได้ทุกเมื่อ รูปต่อไปเป็นการแนะนำเกี่ยวกับการคุกคามจากภายนอก เพราะความผิดพลาดเพียงเล็กน้อยของพนักงาน เช่น ไม่ได้ปิดประตูหน้าต่างทำให้หัวขโมยเข้ามาในองค์กรได้ การลบหรือแก้ไขข้อมูลที่เป็นเอกสารสำคัญ

2. การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property)

ทรัพย์สินทางปัญญา (IP) เป็นส่วนหนึ่งของการดำเนินธุรกิจ ซึ่งทรัพย์สินทางปัญญา เป็นผลงานของผู้ที่เป็นเจ้าของความคิด และเป็นทรัพย์อีกชนิดหนึ่ง ได้แก่ ลิขสิทธิ์ เครื่องหมายการค้าและสิทธิบัตร คุณสมบัติของทรัพย์สินทางปัญญาอย่างหนึ่งคือ มีการระบุรหัสบ่งชี้ไว้อย่างเหมาะสมบ่อยครั้งที่องค์ซื้อหรือทำสัญญาเช่าทรัพย์สินทางปัญญาจากองค์กรอื่น ต้องปฏิบัติตามข้อตกลงที่ได้ทำไว้เพื่อความยุติธรรมและความรับผิดชอบในการนำไปใช้ ส่วนใหญ่การละเมิดทรัพย์สินทางปัญญาจะเป็นการทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์ซึ่งเป็นการกระทำที่ผิดกฎหมายผู้ผลิตซอฟต์แวร์ใช้เทคนิควิธีในการควบคุม เพื่อป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์นอกเหนือจากกฎหมายต่อต้านการละเมิดลิขสิทธิ์ซอฟต์แวร์ ยังมี 2 องค์กร ที่คอยเฝ้าระวังการละเมิดลิขสิทธิ์คือ SIIA, BSA เมื่อเร็วๆ BSA สำรวจเมื่อเดือนพฤษภาคม 2006 เปิดเผยว่าเศษหนึ่งส่วนสามของซอฟต์แวร์ที่ใช้ในโลกเป็นซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ องค์กรเหล่านี้แสดงรายละเอียด และวิธีปฏิบัติ เพื่อป้องกันการละเมิดสิทธิ์ในทรัพย์สินทางปัญญา และมีเทคนิควิธีจำนวนมากที่ใช้ตรวจสอบเช่น ลายน้ำดิจิตอล การฝังรหัสลิขสิทธิ์ เป็นเจตนาทำให้เกิด bad sectors บนสื่อที่บรรจุซอฟต์แวร์เพื่อให้มีการปฏิบัติตามกฎหมายลิขสิทธิ์

3. การบุกรุก (Deliberate Acts of Trespass)

การบุกรุกจากภายนอกเป็นสิ่งที่ได้รับการกล่าวถึงอย่างมาก ทั้งในรูปแบบที่เป็นอิเลคทรอนิกส์และกระทำโดยคนที่สามารถเข้าถึงข้อมูลที่เป็นความลับ เมื่อมีบุคคลที่ไม่ได้รับอนุญาตได้ทำการรุกล้ำและพยายามเข้าถึงข้อมูลขององค์กรที่มีการป้องกัน ซึ่งพฤติกรรมดังกล่าวเป็นการบุกรุกโดยเจตนานักโจมตีระบบสามารถที่จะใช้วิธีการต่าง 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, รหัสผ่านขอเครื่องโทรศัพท์ขณะที่มีการทำรายการผ่านทางโทรศัพท์ เป็นต้นโดยปกติไม่ได้มีการเขียนเป็นข้อบังคับหรือข้อห้ามโดยชัดเจนในการแอบดูข้อมูลความเป็นส่วนตัวของผู้อื่น เนื่องจากถือเป็นมรรยาทที่

ทุกคนควรปฏิบัติโดยปกติอยู่แล้ว ดังนั้นเจ้าของข้อมูลที่เป็นส่วนตัวจะต้องป้องกันตนเองเป็นอันดับแรกจากภัยคุกคามในรูปแบบนี้

Hacker นักเจาะระบบที่มีความเชี่ยวชาญในการเขียนโปรแกรมที่สามารถจะเข้าถึงข้อมูลที่มีการป้องกันอย่างผิดกฎหมาย ซึ่งโดยส่วนใหญ่จะเป็นการกระทำเพื่อทดสอบความสามารถของตนเองชอบสิ่งที่ท้าทายหรือลี้ลับที่ต้องการค้นหา โดยการทุ่มเทเวลาในการเขียนโปรแกรม โดยใช้ความรู้ที่มีอยู่และค้นคว้าเพิ่มเติม ในการที่พยายามจะเจาะระบบที่มีการรักษาความปลอดภัยที่แน่นหนา เป็นเป้าหมายหลัก

วิวัฒนาการของ Hacker (Hacker profiles)

ในยุคแรก ๆ Hacker ส่วนมากจะเป็นเพศชาย มีอายุระหว่าง 13-18 ปี ซึ่งขาดการดูแลเอาใจใส่จากผู้ปกครอง และใช้เวลาส่วนใหญ่อยู่กับการใช้เครื่องคอมพิวเตอร์ในปัจจุบัน Hacker จะไม่มีการจำกัดเพศและมีช่วงอายุที่เปลี่ยนไปคือ ระหว่าง 12-60 ปี ประวัติหรือภูมิหลังไม่เป็นที่รู้จัก เนื่องจากความเปลี่ยนแปลงทางเทคโนโลยี ระดับความรู้ต่าง ๆ และHacker อาจจะเป็นบุคคลจากภายในหรือภายนอกองค์กรก็ได้

ประเภทของ Hacker ตามระดับความสามารถ แบ่งได้ออกเป็น 2 กลุ่ม คือ

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

Expert Hacker

ส่วนใหญ่จะเป็นผู้ที่มีทักษะขั้นสูงในการเขียนโปรแกรมได้หลากหลายภาษารวมถึงความรู้เกี่ยวกับการทำงานของระบบเครือข่ายและระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ และมีคุณลักษณะพิเศษคือ มีความกระตือรือร้นและทุ่มเทเวลา ในการพยายามที่จะเจาะระบบความปลอดภัยขั้นสูงของผู้อื่น ดังนั้นเมื่อกลุ่มเป้าหมายที่ถูกเลือกแล้วมีโอกาสหรือความเป็นไปได้สูงที่ระบบความปลอดภัยจะถูกบุกรุกหรือคุกคามโดย Expert Hacker ในการโจมตีหรือเจาะระบบจะมีการประกาศหรือแจ้งให้รู้โดยตรงด้วยการเขียนไว้ในโปรแกรมที่ใช้ในการบุกรุกระบบ

Novice Hacker

เป็น Hacker ที่มีความรู้หรือทักษะในการเขียนโปรแกรมจำกัดและไม่สามารถที่จะพัฒนาโปรแกรมที่เจาะระบบได้เหมือนกับ Expert Hacker จะเป็นการใช้โปรแกรม Hackสำเร็จรูปที่เขียนขึ้นโดย Expert Hacker มาเป็นเครื่องมือในการโจมตีระบบรักษาความปลอดภัยอีกทีหนึ่ง เรียกว่า Script Kiddies หรือ Packet Monkey โดยที่ Novice Hacker จะไม่สามารถทราบถึงกลไกหรือกระบวนการทำงานภายในโปรแกรม Script Kiddies จะเป็นลักษณะการโจมตีที่ก่อกวนเครือข่ายคอมพิวเตอร์เป็นส่วนใหญ่ (Denial-of-service) Novice Hacker สามารถหาโปรแกรมที่เป็นScript Kiddies โดยการ Download จาก Internet ซึ่ง Expert Hacker นำไปเผยแพร่ไว้ ในทางกลับกันผู้ดูแลรักษาความปลอดภัยของระบบก็สามารถที่จะค้นพบ

โปรแกรมเหล่านี้ได้เช่นกัน ทำให้เกิดนักพัฒนาโปรแกรมหรืออุปกรณ์ที่นำมาใช้ป้องกันระบบจากการโจมตีหรือการบุกรุกจากภายนอกในเดือนกุมภาพันธ์ ปี 2000 มี Hacker หนุ่ม ที่ใช้ชื่อว่า Mafiaboy ถูกจับเนื่องจากเข้าไปโจมตีและก่อกวนระบบเครือข่ายของ Web site โดยถูกตัดสินให้จำคุก 8 เดือน และ ถูกปรับเป็นเงิน 250 ดอลล่าร์ บริจาคให้การกุศล สาเหตุที่ทำให้ต้องถูกจับเนื่องจากไม่สามารถที่จะลบ System Logsที่ตรวจจับการกระทำการบุกรุกของ Mafiaboy และจากการที่ได้ไปแสดงตัวหรือโอ้อวดถึงการกระทำดังกล่าวในห้องสนทนาทางอินเตอร์เน็ต

Cracker

จะเป็นการถอดรหัสหรือทำลายโปรแกรมที่ใช้ในการป้องกันการทำข้อมูลซ้ำ ซึ่งเป็นการกระทำที่ละเมิดลิขสิทธิ์โปรแกรมประเภท Cracker สามารถที่จะเผยแพร่และติดตั้งได้อย่างง่ายดายความหมายของ Hacker และ Cracker จะพิจารณาจากเจตนาของกระทำความผิดเป็นหลักHacker 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

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 ส่งผลกระทบต่อความเชื่อมั่น ของลูกค้าทำให้ยอดขายและมูลค่าขององค์กร รวมถึงชื่อเสียงก็ลดลงเช่นกัน

6. การโจรกรรม (Deliberate Acts of Theft)

การคุกคามโดยการโจรกรรม จากบุคคลที่ได้มีการไตร่ตรองไว้ล่วงหน้า โดยมีเจตนายึดทรัพย์สินของผู้อื่นไปครอบครองโดยผิดกฎหมาย ซึ่งภายในองค์กรสามารถถูกโจรกรรมทรัพย์สินดังต่อไปนี้ ทรัพย์สินทางกายภาพ (Physical Property) เช่น เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์เป็นต้น

แนวทางการป้องกัน

- การตรวจนับจำนวนทรัพย์สินสม่ำเสมอ
- ทำการล็อคประตูและมีการจัดอบรมเจ้าหน้าที่ด้านความปลอดภัย
- ติดตั้ง ระบบสัญญาณเตือนภัย

ทรัพย์สินทางอิเล็กทรอนิกส์ (Electronic Property) มีความซับซ้อนในการจัดการและควบคุมซึ่งเป็นปัญหาขององค์กร ซึ่งต่างจากการโจรกรรมทรัพย์สินทางกายภาพสามารถตรวจพบได้ง่ายกว่าเมื่อทรัพย์สินทางอิเล็กทรอนิกส์ถูกขโมยไป องค์กรส่วนใหญ่จะทราบว่าทรัพย์สินถูกโจรกรรมมักจะสายเกินไป เนื่องจากนักโจรกรรมได้ทำการปกปิดร่องรอยการกระทำความผิดอย่างระมัดระวังทรัพย์สินทางปัญญา (Intellectual Property) มูลค่าของข้อมูลจะลดน้อยลง ถ้าถูกขโมยไปโดยปราศจากความรู้ของเจ้าของทรัพย์สิน

7. การโจมตีซอฟต์แวร์ (Deliberate Software Attacks)

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

Virus

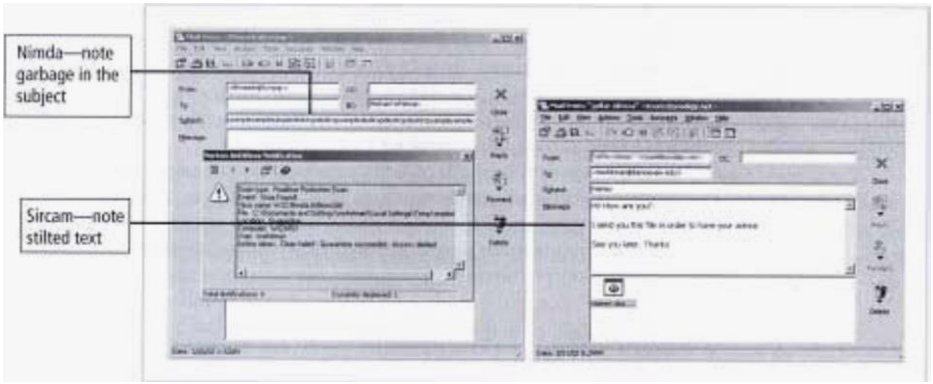
ไวรัสคอมพิวเตอร์ประกอบด้วยส่วนของโค๊ดทำหน้าที่มุ่งร้าย ซึ่งโค๊ดนี้จะทำตัวคล้ายกับเชื้อไวรัสที่โจมตีสัตว์และพืช โดยสามารถแพร่กระจายได้ด้วยตัวเอง คอมพิวเตอร์ที่มีโปรแกรมไวรัสอยู่ไวรัสจะเข้าไปควบคุมการทำงานของคอมพิวเตอร์ให้ทำงานผิดปกติ และแพร่กระจายไวรัสเข้าไปในระบบ บ่อยครั้ง ผู้ใช้ทำให้ไวรัสเข้าสู่ระบบโดยรู้เท่าไม่ถึงการณ์ เช่น การเปิดอีเมล์ หรือการสุ่มส่งป๊อปอัพไป หากผู้ใช้ไม่ตรวจสอบไฟล์ที่ได้รับแล้วเปิดอ่านเลย ข้อมูลและฮาร์ดไดร์จะถูกทำลายทั้งหมดไวรัสสามารถส่งผ่านจากเครื่องหนึ่งไปสู่อีกเครื่องได้ผ่านสื่อต่างๆ อีเมล์ หรือการส่งข้อมูลทางคอมพิวเตอร์ เมื่อเครื่องติดไวรัสแล้วมันจะแพร่กระจายไปกับอีเมล์ หรือการส่งไปยังผู้ใช้ทุกคนที่มีชื่ออยู่ในสมุดที่อยู่

วิธีที่ใช้มากที่สุดในการส่งไวรัสในศตวรรษที่21 คือการแนบไฟล์ไปกับอีเมล์ องค์กรจำนวนมากป้องกันอีเมล์ด้วยการเลือกอีเมล์ที่ไว้ใจได้ และการกรองอีเมล์ทั้งหมดซึ่งรู้ว่าอีเมล์ใดมีไวรัสบ้าง ไวรัสใช้เวลาเพียงเล็กน้อยในการติดตั้งโปรแกรมไวรัสด้วยแผ่นดิสก์แล้วกระจายไปยังระบบต่างๆปัจจุบันเครือข่ายคอมพิวเตอร์และโปรแกรมตรวจสอบอีเมล์ เพื่อจัดการไวรัสมีอยู่มาก ผู้จำหน่ายซอฟต์แวร์ป้องกันไวรัสที่

ได้รับการยอมรับมีดังนี้ Symantec Norton Anti-Virus และ McAfeeVirusScan มีโปรแกรมช่วยในการจัดการไวรัสคอมพิวเตอร์ได้ในจำนวนชนิดของไวรัสคอมพิวเตอร์ในระบบเป็นไวรัสที่เขียนขึ้นมาเอง (macro virus) ด้วยการฝังชุดคำสั่ง ลงไปที่ระบบปฏิบัติการของเครื่องคอมพิวเตอร์โดยอัตโนมัติ เมื่อมีการใช้โปรแกรมเวิร์ด เอ็กเซลล์ และระบบฐานข้อมูล ไวรัสจะเริ่มทำงาน ซึ่งไฟล์ของระบบปฏิบัติการจะติดไวรัสที่ชุดคำสั่งในการเปิดเครื่อง (boot sector)

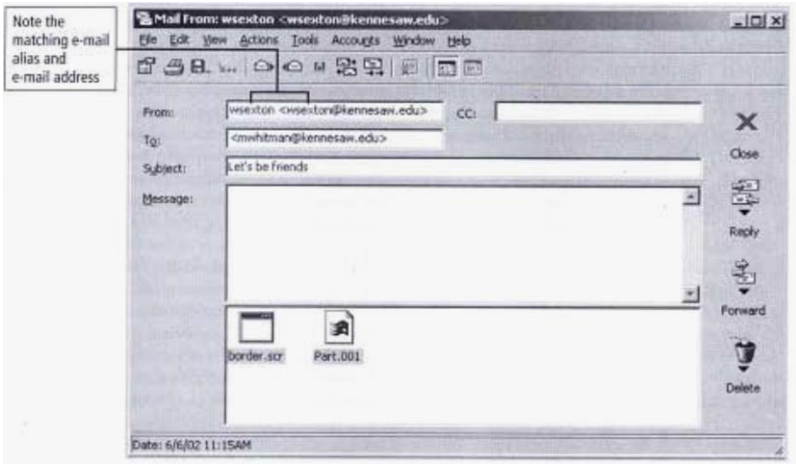
Worms

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

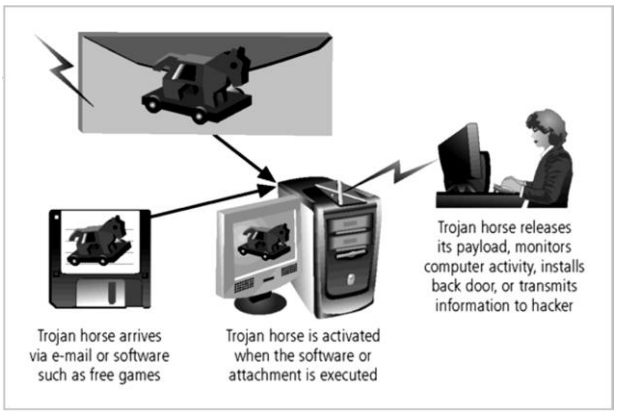
เวิร์มมีการเปลี่ยนแปลงรูปแบบการแพร่กระจายตัวเองจำนวนมากดังรูปข้างล่าง เป็นแบบdouble-barreled payload ซึ่งเวิร์มจะส่งเมล์จำนวนมากและแนบตัวเองไปกับอีเมล์ด้วย เวิร์มที่มีการจู่โจมแบบแพร่กระจายนี้ได้แก่ MS-Blaster, MyDoom และ Netsky โดยเวิร์มและไวรัสมีการเปลี่ยนแปลงการโจมตีจุดอ่อนของระบบปฏิบัติการและแอพพลิเคชัน่ ได้หลายรูปแบบ



รูปแสดง Klez Virus

Trojan horses

โทรจันฮอร์สจะแฝงตัวมากับซอฟต์แวร์ จะทำงานเมื่อผู้ใช้รันซอฟต์แวร์ แล้วโทรจันฮอร์สจะทำลายระบบคอมพิวเตอร์ เช่น เมื่อเรียกไฟล์ .exe ที่มากับแชร์แวร์ หรือ ฟรีแวร์รูปแสดงตัวอย่างสรุปการโจมตีของโทรจันฮอร์ส ประมาณ 20 มกราคม 1999 เริ่มจากผู้ใช้ได้รับอีเมล์ที่มีโปรแกรมโทรจันฮอร์สแนบมาชื่อ Happy99.exe เมื่อเปิดอีเมล์และติดตั้งโปรแกรมโทรจันฮอร์สที่แฝงมาจะก่อกวนระบบทันที เช่น ลบไฟล์ หรือ สร้างแบ็คดอร์ให้แฮคเกอร์เข้ามาขโมยข้อมูลลบไฟล์ต่างๆในระบบได้



รูปแสดง Trojan Horse Attack

Virus and Worm Hoaxes

เป็นรูปแบบของการหลอกลวงผู้ใช้คอมพิวเตอร์ทำให้เสียเงินเสียเวลาในการวิเคราะห์ โดยไวรัสหลอกลวงจะมาในรูปจดหมายอิเล็กทรอนิกส์ เตือนให้ระวังอันตรายจากไวรัส ด้วยการอ้างแหล่งข้อมูลเป็นรายงานที่น่าเชื่อถือ เพื่อให้ผู้รับส่งต่อจดหมายเตือนฉบับนั้นต่อๆไปอีกหลายๆทอดซึ่งเป็นลักษณะของไวรัส

หลอกลวง หากได้รับจดหมายประเภทนี้ไม่ควรที่จะส่งต่อ ควรเช็คจากแหล่งข้อมูลที่ถูกต้องก่อนทำการส่ง และควรจะอัพเดทโปรแกรมแอนตี้ไวรัสอย่างสม่ำเสมอ

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

8. ภัยธรรมชาติ (Forces of Nature)

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

o Fire: ไฟไหม้ สร้างความเสียหายต่ออุปกรณ์ทางคอมพิวเตอร์ รวมถึงระบบสารสนเทศต่างๆ เนื่องจากควันไฟ และน้ำ ซึ่งเกิดจากการดับไฟของนักดับเพลิง ภัยจากไฟไหม้สามารถบรรเทาได้ด้วยการทำประกันอุบัติภัย เพื่อเป็นการลดความเสียหายที่เกิดขึ้นต่อทรัพย์สิน และชีวิต หรือทำประกันภัยธุรกิจ หากธุรกิจต้องหยุดดำเนินกิจการ

o Flood: น้ำท่วม เป็นสาเหตุโดยตรงที่สร้างความเสียหายต่อระบบสารสนเทศ หรือในส่วนของอาคารระบบสารสนเทศ น้ำท่วมทำให้การเข้าใช้อาคารสถานที่ หรือในส่วนการทำงานของระบบสารสนเทศติดขัด ภัยคุกคามนี้สามารถบรรเทาได้ด้วยการทำประกันอุทกภัยหรือประกันภัยธุรกิจ

o Earthquake: แผ่นดินไหว เกิดจากการเคลื่อนตัวของเปลือกโลกกะทันหัน เป็นความเสียหายทางธรณีวิทยาจากการเกิดภูเขาไฟระเบิด แผ่นดินไหวสร้างความเสียหายต่อทุกส่วนของระบบสารสนเทศ บ่อยครั้งสร้างความเสียหายกับอาคารเป็นการขัดขวางการเข้าใช้ระบบสารสนเทศ สามารถบรรเทาภัยคุกคามนี้ได้ด้วยการทำประกันภัยพิเศษ หรือ การประกันภัยธุรกิจ ทั้ง นี้จะเลือกรูปแบบใดขึ้นอยู่กับการกำหนดนโยบายที่ต่างกัน

o Lightning: ฟ้าแลบ เป็นกระแสไฟฟ้าทางธรรมชาติที่ถูกปลดปล่อยออกมารบกวนคลื่นวิทยุ ฟ้าผ่าสร้างความเสียหายต่อระบบสารสนเทศ หรือ ส่วนของการจ่ายไฟ ทำให้ไฟดับ หรือ สร้างปัญหาในการใช้สถานที่ทำงานเนื่องจากไม่มีกระแสไฟฟ้า หรือ สร้างความยุ่งยากในการปฏิบัติงาน

o Landslide or mudslide: แผ่นดินถล่ม หรือ โคลนถล่ม เกิดจากดินและหินจำนวนมากไหลจากที่สูงสร้างความเสียหายต่อระบบสารสนเทศ ทั้งในส่วนของการเข้าใช้อาคารสถานที่และการเข้าใช้ระบบสารสนเทศ ซึ่งภัยคุกคามนี้สามารถบรรเทาความเสียหายได้ด้วยการทำประกันภัย หรือ การประกันภัยธุรกิจ

เนื่องจากภัยคุมคามทางธรรมชาติไม่อาจที่จะหลีกเลี่ยงได้ องค์กรต้องเพิ่มการควบคุมที่จะจำกัดความเสียหาย และต้องวางแผนกับความไม่แน่นอนสำหรับการปฏิบัติงานอย่างต่อเนื่อง เช่นแผนการกู้ข้อมูลวางแผนอย่างต่อเนื่อง และแผนการรับมือกับเหตุการณ์ที่อาจเกิดขึ้นโดยบังเอิญ เพื่อจำกัดความเสียหายจากภัยคุกคามเหล่านี้

ATTACKS

การโจมตีเป็นการกระทำเพื่อให้เกิดความไม่มั่น คงและเป็นอันตรายต่อการควบคุมระบบคอมพิวเตอร์ โดยเป้าหมายของการโจมตีเพื่อสร้างความเสียหายหรือการขโมยข้อมูลที่สำคัญขององค์กร ในส่วนนี้จะเป็นการอธิบายแต่ละประเภทของการโจมตีระบบที่สำคัญๆ

Spam

เป็นอีเมล์ที่เราไม่ต้องการ จุดประสงค์ของผู้ส่ง Spam Mail เพื่อต้องการโฆษณาและบริการต่างๆ สำหรับ Spam Mail จะสร้างความรำคาญให้กับผู้รับอีเมล์มากกว่าจุดประสงค์เพื่อการโจมตี แต่ในเดือนมีนาคม ปี 2002 มีรายงานว่ามีการแนบไวรัส มากับ Spam Mail ด้วยหลายๆ บริษัทพยายามที่จะป้องกัน Spam Mail โดยการที่ใช้เทคโนโลยีในการคัดกรองอีเมล์แต่ก็มีบางบริษัทที่ใช้วิธีแบบง่ายๆ โดยให้ผู้ใช้ลบอีเมล์ที่ไม่ต้องการออกจากระบบอีเมล์ของบริษัทด้วย

Mail Bombing

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

Phishing

การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ (Email Spoofing) และทำการสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password)หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆสามารถทำได้โดยการขโมยหรือนำเครื่องหมายหรือสัญลักษณ์ตลอดจนรูปลักษณ์ของธนาคารหรือสถาบันการเงินที่มีชื่อเสียง และบัตรเครดิตประเภทต่างๆของผู้ประกอบการ การให้สินเชื่อทางอินเตอร์เน็ต มาประกอบเข้ากับการหลอกลวงเหยื่อหรือผู้ใช้ให้เปิดเผยข้อมูล ซึ่งมีการประเมินเบื้องต้นว่า การโจมตีในรูปแบบของ Phishing สามารถหลอกให้เหยื่อร้อยละ 5 ของทั้ง หมด เปิดเผยข้อมูลที่ต้องการ นอกจากนี้ ผู้โจมตี (Hacker หรือ Spammer) ยังใช้ยุทธวิธีการหลอกลวงแบบ Social Engineering ประกอบเพิ่มเติม เพื่อให้มีความน่าเชื่อถือยิ่งขึ้น เช่น การหลอกลวงชื่ออี-เมล์ เป็นต้นว่าเป็นเรื่องด่วนจากธนาคาร การหลอกลวงว่าบัญชีที่ใช้งานจะหมดอายุ การเสนอสินค้าที่มีดอกเบี้ยต่ำต่างๆ เป็นต้น