HSS :Hacker Surrender Solution

Highlight

จุดเด่น

- ✓ **Complete external protection**
  HSS เป็นกระบวนการป้องกันความเสี่ยงจากภายนอกอย่างสมบูรณ์แบบ
- ✓ **Vender experience**
  HSS ถูกพัฒนาจากผู้ให้บริการที่มีประสบการณ์มากว่า 10 ปี
- ✓ **New protect solution**
  HSS เป็นการคิดแนวใหม่ที่แตกต่างจากระบบเดิมๆ
- ✓ **Reduce business risk, time and cost**
  HSS สร้างมาเพื่อลดความเสี่ยง เวลา และ ค่าใช้จ่าย
- ✓ **Flexible for environment**
  HSS ถูกออกแบบมาให้สอดคล้องกับทุกองค์กร
- ✓ **Manageable & Maintainable**
  HSS เป็น Framework ที่บริหารจัดการได้ง่าย
- ✓ **Global knowledge**
  HSS รวบรวมข้อมูลข่าวสาร และความรู้ของกลุ่มนักคิดระดับโลก
- ✓ **Proactive solution**
  HSS ถูกพัฒนาอย่างต่อเนื่อง เพื่อป้องกันการบุกรุกในอนาคต

Hacker Surrender Solution

ความสำคัญของ Hacker Surrender Solution

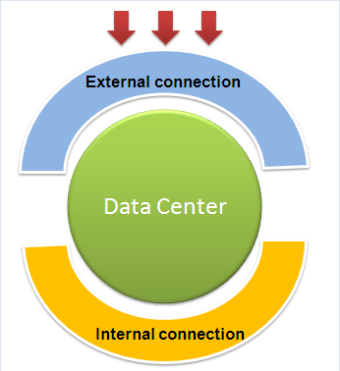
การดำเนินงานทางธุรกิจในปัจจุบันนั้นต่างมุ่งเน้นแข่งขันในการพัฒนาระบบคอมพิวเตอร์เพื่อตอบสนองการทำงานที่สะดวก รวดเร็ว ส่งผลให้แต่ละองค์กรจำเป็นต้องสร้างระบบรักษาความปลอดภัยเพื่อป้องกันการถูกบุกรุกของผู้ไม่หวังดี ซึ่งอาจส่งผลกระทบอย่างร้ายแรงให้กับองค์กร

บริษัท MFEC ร่วมมือกับกลุ่มผู้เชี่ยวชาญ วิจัย และ พัฒนามาตรฐานความปลอดภัยในรูปแบบ Framework ชื่อว่า **"Hacker Surrender Solution (HSS)"** ที่ช่วยสร้างความแข็งแกร่งให้กับระบบเครือข่ายขององค์กร เพื่อให้เกิด**ความปลอดภัยอย่างสมบูรณ์แบบ** โดย HSS ใช้แนวคิดที่แตกต่างจากเดิมทำให้ระบบสามารถรองรับความเสี่ยงในอนาคตได้อย่างต่อเนื่อง เพราะ Hacker มีการพัฒนาอยู่ตลอดเวลา ดังนั้น HSS จะก้าวนำหน้ายิ่งกว่า

Hacker Surrender Solution (HSS) คืออะไร

Hacker Surrender Solution (HSS) เกิดจากกลุ่มผู้เชี่ยวชาญได้ทำการเก็บรวบรวมข้อมูล และวิเคราะห์เส้นทางการบุกรุกจากภายนอก ซึ่งจากการศึกษาวิจัยนั้นทำให้ผู้เชี่ยวชาญสรุปว่าการบุกรุกนั้นเกิดขึ้นจาก 2 สาเหตุหลัก ได้แก่

- **การติดตั้งอุปกรณ์รักษาความปลอดภัยที่ไม่เพียงพอ**
- **การทำงานที่ไม่สอดคล้องกันระหว่างอุปกรณ์รักษาความปลอดภัยที่ได้ติดตั้งในระบบ**



สิ่งที่น่าสนใจคือเมื่อองค์กรติดตั้งอุปกรณ์รักษาความปลอดภัยแล้ว **ทำไมระบบยังถูกบุกรุกได้อีก** ซึ่งผู้เชี่ยวชาญให้ความสนใจและมุ่งเน้นพัฒนากระบวนการเพื่อสร้างความปลอดภัยให้กับระบบเครือข่ายโดยยึดหลักแนวคิดที่ว่า **"ทำอย่างไรให้สามารถสร้างระบบรักษาความปลอดภัยอย่างเพียงพอให้กับเครือข่าย"**

ซึ่งผู้เชี่ยวชาญมุ่งเน้นไปที่การป้องกันการบุกรุกจากภายนอก (External Protection) ส่งผลให้เกิดกระบวนการป้องกันแนวใหม่ โดยมุ่งเน้น**การปรับแต่งให้อุปกรณ์รักษาความปลอดภัยให้ทำงานได้อย่างสอดคล้อง และสร้างกระบวนการรักษาความปลอดภัยในระดับของการควบคุมพฤติกรรม** ส่งผลให้เพิ่มประสิทธิภาพของการป้องกันผู้บุกรุกได้สมบูรณ์ที่สุดในขณะนี้

ทำไมระบบการรักษาความปลอดภัยจากอุปกรณ์จึงไม่เพียงพอ

เนื่องจากระบบรักษาความปลอดภัยของระบบเครือข่ายในปัจจุบันมุ่งเน้นการติดตั้งอุปกรณ์เพื่อรักษาความปลอดภัยเฉพาะด้าน

การทำงานของแต่ละอุปกรณ์นั้นจะทำงานเฉพาะเจาะจงตามหน้าที่ของตนเอง โดยยับยั้งพฤติกรรมที่ไม่ปกติ ("Abnormal" บนพื้นฐาน "Black lists") เป็นลำดับชั้น ซึ่งไม่ครอบคลุมการบุกรุกในปัจจุบัน ทำให้เกิดช่องโหว่หรือรอยรั่วของการรักษาความปลอดภัย (Residual Risk) และผู้บุกรุกอาศัยรอยรั่วหรือช่องโหว่เหล่านี้สร้างเส้นทางการบุกรุก "Hacking route path" เพื่อโจรกรรมข้อมูลหรือทำลายระบบ ซึ่งรอยรั่วเหล่านี้แม้จะเป็นแค่เพียงเล็กน้อย แต่ก็มากเพียงพอที่ผู้บุกรุกสามารถโจมตีระบบเครือข่ายขององค์กรได้

กระบวนการทำงานของ HSS

กระบวนการทำงานของ Hacker Surrender Solution นั้นเป็นการสร้างกระบวนการรักษาความปลอดภัยในรูปแบบที่แตกต่างและนำมาประยุกต์ใช้กับระบบการป้องกันที่องค์กรมีอยู่เดิม โดยมีกระบวนการดังนี้

- ❖ปรับแต่งอุปกรณ์รักษาความปลอดภัยให้ทำงานได้อย่างสอดคล้อง หากอุปกรณ์รักษาความปลอดภัยใดตรวจสอบพฤติกรรมที่อาจจะก่อให้เกิดความเสี่ยงจากการบุกรุก ให้ทำงานร่วมกับอุปกรณ์ที่เกี่ยวข้องเพื่อยับยั้งพฤติกรรมเหล่านั้นออกจากระบบ
- ❖สร้างกระบวนการรักษาความปลอดภัยในระดับของการควบคุมพฤติกรรมการทำงานของ process โดยอนุญาตให้พฤติกรรมที่ถูกต้อง (“White lists”) เท่านั้น จึงสามารถเข้าใช้งานเครือข่ายได้

ทำไม HSS ถึงเพียงพอต่อการรักษาความปลอดภัยของระบบ

การคงความปลอดภัยของระบบนั้นมีความสำคัญอย่างมาก เนื่องจากเทคโนโลยีการบุกรุกถูกพัฒนาไปอย่างรวดเร็ว ซึ่งผู้เชี่ยวชาญคำนึงถึงปัญหานี้ จึงออกแบบกลไก เฝ้าระวังการบุกรุกและการตอบสนองให้ทันท่วงที โดยมี **ทีมผู้เชี่ยวชาญเป็นผู้คอยดูแลระบบเครือข่ายให้กับองค์กร** โดยติดตามวิธีการบุกรุก ช่องโหว่ใหม่ๆ และปรับปรุงการทำงานของอุปกรณ์ให้รู้เท่าทันผู้บุกรุกอยู่เสมอ

กระบวนการดังกล่าวได้ผ่านการวิจัย พัฒนา จากผู้เชี่ยวชาญที่มีประสบการณ์ด้านการรักษาความปลอดภัยระบบเครือข่าย เพื่อสร้างวิธีการป้องกันการบุกรุกในรูปแบบใหม่ๆ ทั้งที่เกิดขึ้นแล้ว และคาดว่าจะเกิดขึ้นในอนาคต ได้รับการสนับสนุนด้านข้อมูลจากเจ้าของผลิตภัณฑ์และงานวิจัยที่เชื่อถือได้ ทำให้ระบบมีความปลอดภัยที่สามารถใช้งานได้จริงและเป็นปัจจุบันเสมอ

หลักการทำงานของ HSS นั้นไม่เพียงแต่ยึดหลักการป้องกันระบบ แต่เน้นให้การจัดการและการดูแลระบบทำได้โดยง่าย (Manageable & Maintainable) โดยสามารถบริหารจัดการระบบได้จากศูนย์กลาง (Centralize management) จึงทำให้สะดวกต่อผู้ใช้งาน และส่งผลให้ระบบปลอดภัยอย่างต่อเนื่อง

HSS ตอบโจทย์การรักษาความปลอดภัยขององค์กรได้อย่างไร

Hacker Surrender Solution ได้ถูกคิดค้น วิจัย พัฒนา กระทั่งออกแบบมาเพื่อช่วยให้การรักษาความปลอดภัยของเครือข่ายในองค์กรสมบูรณ์ที่สุดโดยมีคุณสมบัติดังนี้

- ลดความเสี่ยงของการถูกบุกรุกระบบ กว่า 3600 ความเสี่ยงที่มีมาตั้งแต่ปี 1997
- ติดตั้งง่าย แม้ระบบเครือข่ายที่มีอยู่เดิมจะซับซ้อนเพียงใด
- ลดค่าใช้จ่าย เพราะดำเนินการเสร็จสิ้นภายใน 60 วัน
- ระบบเครือข่ายมีความปลอดภัยอย่างต่อเนื่อง ด้วยบุคคลากรที่มีความสามารถร่วมดูแลระบบ
- เน้นการพัฒนาและถ่ายทอดความรู้ให้กับองค์กร

HSS