SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 2 ฉบับที่ 14 ประจำเดือน มิถุนายน 2553

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

จากอาชญากรรมทางคอมพิวเตอร์ที่เกิดเพิ่มขึ้นอย่างต่อเนื่อง และมีผู้ได้รับความเสียหายติดต่อขอความช่วยเหลือเข้ามาที่โกลบอลเทคฯ หลายราย จดหมายข่าวฉบับนี้จึงขอนำเสนอตัวอย่างเหตุการณ์พร้อมบทวิเคราะห์และแนะนำบริการพิสูจน์หลักฐานการกระทำความผิดทางคอมพิวเตอร์ (Digital Forensics & Investigation Service) มาให้ได้รับทราบกันค่ะ

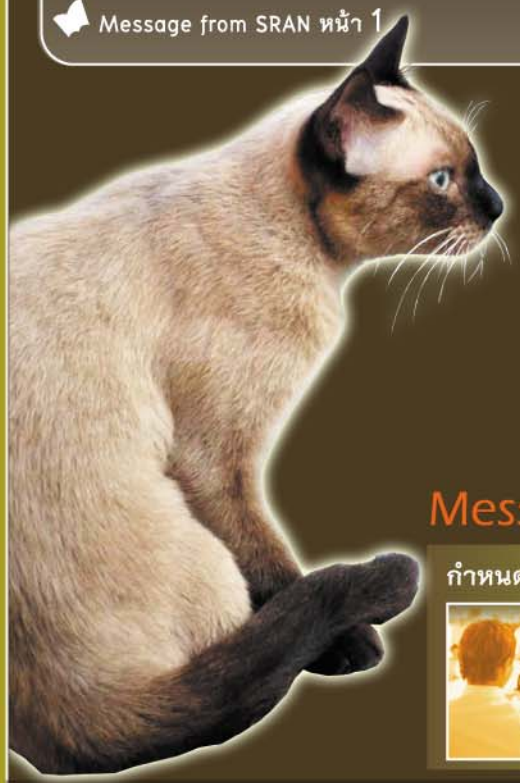
กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- SRAN กับการสืบหาอาชญากรทางคอมพิวเตอร์ หน้า 1–4
- Message from SRAN หน้า 1

SRAN กับการสืบหา... อาชญากรทางคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์นั้น หลายองค์กรอาจมองเป็นเรื่องไกลตัว ไม่น่าจะเกิดขึ้นกับตน จึงมิได้ตระหนักถึงการป้องกันภัยคุกคามทั้งจากภายในและภายนอกองค์กร รวมทั้งการวางระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและมีความปลอดภัย ทำให้บางครั้งเกิดความเสียหายขึ้นอย่างไม่คาดคิด และกระทบต่อผลประกอบการและภาพลักษณ์ขององค์กรอย่างไม่อาจประเมินค่าได้....



Message from SRAN

กำหนดการฝึกอบรมการใช้งาน SRAN **ฟรี!** สำหรับลูกค้าและตัวแทนจำหน่าย ประจำปี 2553

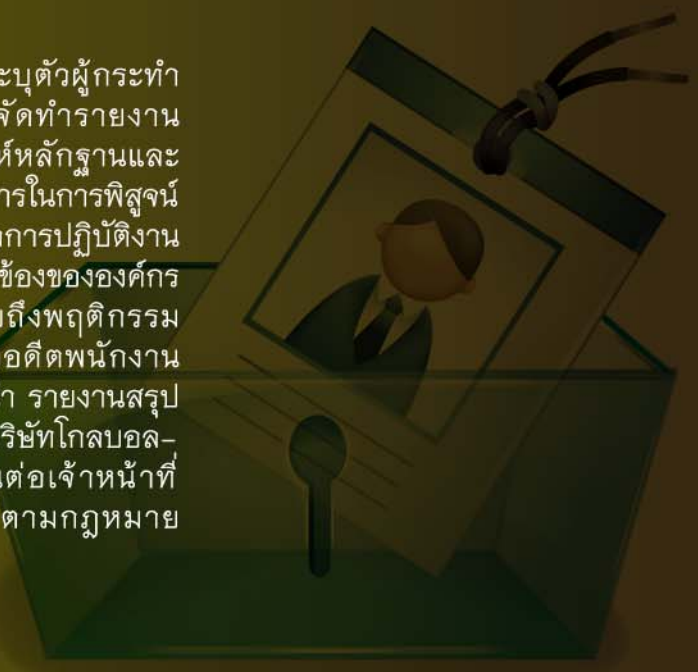
มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
24-25	22-23	26-27	23-24	21-22	25-26	23-24

...และกระทบต่อผลประกอบการและภาพลักษณ์ขององค์กรอย่างไม่อาจประเมินค่าได้ จากประสบการณ์ที่บริษัท โกลบอลเทคโนโลยี อินทิเกรเทด จำกัด ได้ให้คำปรึกษา แนะนำและแก้ไขปัญหาดังกล่าวให้กับหน่วยงานทั้งภาครัฐและเอกชน จึงขอหยิบยกบางตัวอย่างขึ้นมานำเสนอ เพื่อเป็นอุทธาหรณ์ให้เกิดความตระหนักในเรื่องความปลอดภัยข้อมูลสารสนเทศอย่างแพร่หลายยิ่งขึ้น

SRAN กับการสืบหาอาชญากรทางคอมพิวเตอร์

องค์กรแห่งหนึ่ง ซึ่งมีชื่อเสียงและได้รับการยอมรับจากสังคมว่าเป็นองค์กรที่มีอนาคตสดใสในแวดวงธุรกิจเดียวกัน เนื่องจากกลุ่มผู้บริหารที่มีวิสัยทัศน์ ประกอบกับบริษัทมีนโยบายในการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการดำเนินงานและการให้บริการ ปัจจัยดังกล่าวส่งผลให้องค์กรมีอัตราการเติบโตอย่างก้าวกระโดด และด้วยการลงทุนและการให้ความสำคัญต่อการนำระบบเทคโนโลยีสารสนเทศมาใช้อย่างต่อเนื่องจึงทำให้หลายฝ่ายคาดการณ์ว่าองค์กรนี้จะเติบโตและก้าวขึ้นมาเป็นผู้นำในวงการธุรกิจเดียวกัน แต่ปัญหาทางเศรษฐกิจที่ทั่วโลกต้องประสบทำให้องค์กรต้องมีการปรับเปลี่ยนแผนงานหลายๆ ด้านรวมไปถึงการปรับลดจำนวนพนักงานในบางแผนกลง ซึ่งกลายเป็นจุดเริ่มต้นของปัญหาที่ส่งผลกระทบต่อองค์กรเป็นอย่างมาก เนื่องจากพนักงานฝ่ายลูกค้าสัมพันธ์ผู้หนึ่งซึ่งถูก องค์กรยกเลิกสัญญาการจ้างเกิดความคับแค้นใจและได้กลับเข้ามาในองค์กร และล็อคอินเข้าสู่ระบบด้วยชื่อบัญชี (Username) ของตนทำการสำเนา (Copy) ข้อมูลรายชื่อลูกค้าขององค์กรซึ่งเป็นไฟล์ Microsoft Excel (.xls) ที่อยู่ในระบบเซิร์ฟเวอร์ จากนั้นบุคคลดังกล่าวได้ทำการติดต่อลูกค้าและจูงใจให้ลูกค้ายกเลิกสัญญาต่างๆ กับองค์กรเดิมของตน โดยใช้วิธีสร้างเรื่องและกล่าวหาให้ร้ายองค์กรเป็นเหตุให้ลูกค้าบางส่วนเกิดความกังวลและยกเลิกสัญญาในที่สุด สร้างความเสียหายต่อสถานะทางการเงินและภาพลักษณ์ขององค์กรเป็นอย่างมาก

เมื่อบริษัท โกลบอลเทคโนโลยีฯ ได้รับทราบปัญหาดังกล่าวจึงได้ส่งเจ้าหน้าที่แผนกสืบสวนและหาหลักฐานการกระทำผิดทางระบบคอมพิวเตอร์ (Computer Forensic Investigator) เข้าไปตรวจหาหลักฐานการกระทำผิดทางระบบคอมพิวเตอร์ จากนั้นทีมงานของโกลบอลเทคฯ ได้ตรวจสอบและดำเนินการตามขั้นตอนการเก็บและพิสูจน์หลักฐานตามมาตรฐานสากล ตลอดจนวิเคราะห์ข้อมูลการกระทำที่เชื่อมโยงกันตามห่วงโซ่ของเหตุการณ์ (Chain of Events) จนสามารถระบุตัวผู้กระทำความผิดได้ โดยได้จัดทำรายงานสรุปผล การวิเคราะห์หลักฐานและเอกสารบันทึกกระบวนการในการพิสูจน์หลักฐานและนำเสนอผลการปฏิบัติงานต่อผู้บริหารและผู้ที่เกี่ยวข้องขององค์กร เมื่อองค์กรได้รับทราบถึงพฤติกรรมและการกระทำผิดของอดีตพนักงานผู้นั้นแล้ว องค์กรจึงได้นำ รายงานสรุปที่ได้รับจากทีมงานของบริษัทโกลบอลเทคโนโลยีฯ ไปยืนยันต่อเจ้าหน้าที่ตำรวจเพื่อดำเนินคดีตามกฎหมายต่อไป



เมื่อเจ้าหน้าที่ตำรวจสามารถจับกุมอดีตพนักงานผู้ขโมยข้อมูลองค์กร และดำเนินการฟ้องร้องในชั้นศาลแล้ว ทางเจ้าหน้าที่ตำรวจได้ยื่นหลักฐานการพิสูจน์หลักฐาน ทั้งรายงานสรุปผลการวิเคราะห์หลักฐาน ตลอดจนเอกสารบันทึกกระบวนการต่างๆ เพื่อใช้ยืนยันว่าทั้งอุปกรณ์ บุคลากร และกระบวนการในการพิสูจน์หลักฐานของบริษัทโกลบอลเทคโนโลยีฯ นั้นมีการดำเนินการถูกต้องตามมาตรฐานที่ศาลรับรอง หลังจากการพิจารณาคดีสิ้นสุด ผู้พิพากษาได้มีคำตัดสินให้อดีตพนักงานรับโทษตามกฎหมาย เนื่องจากหลักฐานที่นำเสนอต่อศาลนั้นสามารถพิสูจน์การกระทำผิดของอดีตพนักงานได้แน่นหนา ทำให้อดีตพนักงานคนดังกล่าวต้องรับโทษตามพระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

การพิสูจน์หาหลักฐานการกระทำผิดทางคอมพิวเตอร์คืออะไร?

และช่วยเหลือองค์กรได้อย่างไร?

การพิสูจน์หาหลักฐานการกระทำผิดทางคอมพิวเตอร์ (Computer Forensics) นั้นคือกระบวนการสืบสวนหาหลักฐานต่างๆ ที่ อยู่ในระบบคอมพิวเตอร์และนำมาเชื่อมโยงกันตามห่วงโซ่ของเหตุการณ์ (Chain of Events) ซึ่งต้องอธิบายได้ว่า ใคร (Who) ทำอะไร (What) ที่ไหน (Where) เมื่อไหร่ (When) และทำไม / อย่างไร (Why/How) โดยกระบวนการในการพิสูจน์หลักฐานนั้น จะต้องมีมาตรฐานและมีการจัดทำเอกสารประกอบในทุกกระบวนการที่ได้ปฏิบัติงาน

SRAN กับการสืบหาอาชญากรทางคอมพิวเตอร์

เหตุใดอดีตพนักงานจึงสามารถเข้าถึงข้อมูลได้ ทั้งที่ถูกเลิกจ้างไปแล้ว?

จากข้อมูลข้างต้น เป็นที่ทราบกันว่าปัญหาดังกล่าวเกิดขึ้นจากการที่อดีตพนักงานที่ถูกเลิกจ้าง ได้ขโมยข้อมูลลูกค้าขององค์กรไปใช้ในทางมิชอบ โดยสาเหตุที่อดีตพนักงานสามารถขโมยข้อมูลออกไปได้นั้น...

เนื่องจากองค์กรดังกล่าวมีนโยบายในการใช้เทคโนโลยีสารสนเทศในการดำเนินงานภายในองค์กร ซึ่งรวมไปถึงส่วนของการติดต่อลูกค้าและการบริการ โดยได้มีการจัดทำฐานข้อมูลลูกค้าด้วย Microsoft Excel และจัดเก็บไว้ในเซิร์ฟเวอร์ โดยมีพนักงานผู้เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงข้อมูลดังกล่าวได้ โดยต้องมีการล็อคอินด้วย Username และ Password ของตนเองก่อนเข้าใช้งาน แต่ด้วยการขาดการบริหารจัดการนโยบายด้านความปลอดภัยที่ดี ทำให้องค์กรไม่ได้ยกเลิกสิทธิ์การใช้งาน Username ของอดีตพนักงานที่กระทำผิด จึงทำให้อดีตพนักงานคนดังกล่าวสามารถเข้าถึงข้อมูล และนำไปใช้ในทางมิชอบได้

เป็นที่ทราบกันดีว่าในปัจจุบันปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตมีอัตราที่สูงขึ้นอย่างต่อเนื่อง แม้จะมีอุปกรณ์ด้านความปลอดภัยมากมายหลายชนิดถูกนำเสนอออกสู่ตลาดเพื่อใช้ป้องกันปัญหาดังกล่าว แต่การติดตั้งอุปกรณ์ประเภทไฟร์วอลล์หรือ IDS/IPS ก็ไม่อาจทำให้มั่นใจได้ว่าองค์กรของเราจะปลอดจากภัยคุกคามที่มีอยู่รอบด้าน ทั้งภายในและภายนอกองค์กร อีกทั้งปัญหาการก่ออาชญากรรมทางระบบคอมพิวเตอร์ที่เกิดขึ้นกับองค์กรนั้นส่วนใหญ่เกิดจากบุคลากรภายใน ขององค์กรนั้นเอง ประกอบกับการใช้เทคโนโลยีเครือข่ายที่พัฒนาขึ้นอย่างรวดเร็ว ทำให้การเข้าถึงข้อมูลที่เป็นความลับภายในองค์กรสามารถกระทำได้อย่างง่ายดาย หากองค์กรนั้นๆ ไม่ได้มีการวางนโยบายรักษาความปลอดภัยในข้อมูลและระบบสารสนเทศที่ดี

ด้วยเหตุนี้ การลงทุนติดตั้งระบบป้องกันภัยต่างๆ เพียงอย่างเดียวจึงไม่สามารถช่วยให้องค์กรปลอดภัยได้ และอุปกรณ์เหล่านั้นแทบจะไม่มีประโยชน์เลย หากการก่ออาชญากรรมนั้นเกิดจากบุคลากรหรือพนักงานภายในองค์กรเอง ด้วยเหตุนี้ องค์กรจึงควรมีการกำหนดนโยบายรักษาความปลอดภัยด้านข้อมูลสารสนเทศ ซึ่งหากการกำหนดนโยบายเป็นไปอย่างมีประสิทธิภาพ

SRAN กับการสืบหาอาชญากรทางคอมพิวเตอร์

ก็จะช่วยให้องค์กรสามารถควบคุมและป้องกันการก่อความเสียหาย จากผู้ไม่ประสงค์ดีทั้งจากภายในและภายนอกองค์กรได้ดียิ่งขึ้น ขณะเดียวกันเมื่อเกิดความเสียหายขึ้นแล้ว วิธีการแก้ไขที่เหมาะสมที่สุดคือองค์กรควรดำเนินคดีกับผู้กระทำความผิดเหล่านั้น โดยหนทางได้มาซึ่งหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิดนั้นก็คือการพิสูจน์หาหลักฐาน การกระทำผิดทางคอมพิวเตอร์ (Computer Forensics) ซึ่งเป็นกระบวนการสืบหาหลักฐานการกระทำผิดที่อยู่บนพื้นฐานของระบบคอมพิวเตอร์ โดยทุกขั้นตอนในการปฏิบัติการจะต้องเป็นไปตามมาตรฐานที่ศาลรับรอง เพื่อให้ผลของการวิเคราะห์หลักฐานนั้นสามารถนำไปใช้เป็นหลักฐานในชั้นศาล เพื่อยื่นฟ้องดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้

โกลบอลเทคฯ ที่ปรึกษามืออาชีพด้านความปลอดภัยข้อมูลสารสนเทศ

จากปริมาณอาชญากรรมทางคอมพิวเตอร์ที่มีอัตราเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยมีผู้ กระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการติดต่อสื่อสารเผยแพร่ข้อมูลใน การกระทำความผิดหรือการกระทำความผิดในรูปแบบอื่นที่อยู่บนระบบคอมพิวเตอร์ บริษัทโกลบอลเทคโนโลยี อินทิเกรเทด จำกัด จึงได้เปิดให้บริการพิสูจน์หลักฐานการกระทำความผิดทางคอมพิวเตอร์ หรือที่ เรียกว่า “Digital Forensics & Investigation Services” (DFI) ซึ่งครอบคลุมการให้บริการ ดังนี้

1. บริการพิสูจน์หาหลักฐานทางดิจิตอลผ่านระบบเครือข่ายคอมพิวเตอร์ (Network Forensics)

2. บริการพิสูจน์หาหลักฐานจากเครื่องคอมพิวเตอร์ (Computer Forensics)

ด้วยเครื่องมือที่ทันสมัยและทีมงาน มืออาชีพที่มากด้วยประสบการณ์และมีความเชี่ยวชาญ มีผลงานเป็นที่ยอมรับ จากหน่วยราชการหลายแห่ง อาทิสำนักงานตำรวจแห่งชาติ, กระทรวงไอซีที ทั้งยังช่วยประสานข้อมูลกับหน่วยงานต่างๆ ที่เกี่ยวข้องเพื่อช่วยอำนวยความสะดวกในการสืบหาผู้กระทำความผิดและดำเนินคดี ได้อีกด้วย

บริษัท โกลบอลเทคโนโลยีฯ ยินดีให้คำปรึกษาและแก้ไขปัญหาที่เกี่ยวข้องกับความปลอดภัยข้อมูลสารสนเทศ สามารถสอบถามรายละเอียดเพิ่มเติมเกี่ยวกับผลิตภัณฑ์และบริการของบริษัทได้ที่

e-mail : info@gbtech.co.th
โทร. 02-982-5445

และศึกษาข้อมูลเพิ่มเติมได้ที่
www.gbtech.co.th ,
www.sran.net