Orion Investigations
20th Floor, Unit 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

ทำไมการทำ Computer Forensics จึงมีความสำคัญต่อองค์กรของคุณ

February 2012

Date: 02-02-2012

Author: Andrew Smith

Contents

เกี่ยวกับผู้เขียน

Andrew Smit-ผู้อำนวยการแผนก Computer Forensics

แอนดรูว์รับผิดชอบในส่วนของผู้จัดการด้านพิสูจน์หลักฐานทางคอมพิวเตอร์ รวมไปถึงพัฒนาการทำ Computer Forensics ในประเทศไทยเพื่อให้แน่ใจว่าให้เป็นไปตามมาตรฐานสากลและ ตอบโจทย์ความต้องการของลูกค้า แอนดรูว์เป็นผู้เชี่ยวชาญด้านพิสูจน์หลักฐานทางคอมพิวเตอร์ที่มีประสบการณ์มากมายซึ่งครอบคลุมการพิสูจน์หลักฐานทางคดีอาญา ตรวจสอบมัลแวร์ในองค์กร และการสืบสวนทางคอมพิวเตอร์เกี่ยวกับคดีก่อการร้ายในประเทศอังกฤษ และในโซนยุโรป แอนดรูว์เคยร่วมงานกับตำรวจที่ South Yorkshire ซึ่งแห่งนี้นี่เองที่เขาได้รับการอบรมการทำ Computer Forensics ในขณะเดียวกัน แอนดรูว์ยังทำงานกับภาคเอกชนซึ่งเป็นบรัษัทชั้นนำด้าน computer Forensics ในประเทศอังกฤษอีกด้วย แอนดรู ว์เป็นผู้เชี่ยวชาญด้านฝึกอบรม Computer Forensics ที่มีประสบการณ์มากมายและยังได้เข้าร่วมพัฒนากฎหมายทางด้าน Computer Forensics ในประเทศอังกฤษ ซึ่งได้รับการยอมรับ และยังพัฒนาหลักสูตรการเรียนการสอนในระดับปริญญาตรีและปริญญาโท เป็น

ระยะเวลาเกือบ 10 ปีที่แอนดรูว์สะสมประสบณ์การการทำ Computer Forensics ทำให้เขามีประสบณ์การมากมายในการเป็นผู้เชี่ยวชาญ นอกจากนี้ แอนดรูยังสามารถขึ้นศาลเพื่อเป็นพยานทางด้าน Computer Forensics ในกรณีถูกร้องขอหรือเพื่ออธิบายให้ศาลเข้าใจในขั้นตอนการทำและหลักฐานทที่ค้นพบในคอมพิวเตอร์ของผู้ต้องหาให้เป็นไปตามมาตรฐานสากล

คำแนะนำ

ในโลกที่ก้าวไปอย่างรวดเร็วปัจจุบันองค์กรต้องพึ่งพาเทคโนโลยีมากขึ้นเพื่อให้ทันต่อการแข่งขัน ปัจจุบันลูกค้ าทั่วไปต่างคาดหวังว่า สินค้าหรือ องค์กรต่างๆที่เค้าต้องการหาสินค้าจะต้องมีเวบไซท์ที่น่าสนใจและข้อมูลครบตามความต้องการ ซึ่งสามารถตอบโจทย์ความต้องการของลูกค้าได้เป็นอย่างดีในกรณีที่ต้องการซื้อสินค้าออนไลน์ ซึ่งแน่อนว่าก่อนสั่งสินค้า ลู กค้าต้องมีสิทธ์ในการสอบถามข้อมูลของสินค้า โดยผ่านโปรแกรมแชทที่เจ้าของเวปไซต์เตรียมไว้ให้ และฟังก์ชั่นการทำงานของเวปไซต์อื่นที่น่าสนใจเช่น ดูตัวอย่างสินค้า

ปัจจุบันเทคโนโลยีได้กลายเป็นสิ่งจำเป็นในชีวิตประจำวันของผู้คน โดยส่วนใหญ่เน้นเชื่อมต่อระหว่างอีเมลย์ของตัวเองและสามารถติดต่อกับเพื่อนๆได้ในช่วงเวลาทำงาน

Computer Forensics สำคัญต่องค์กรของคุณอย่างไร ? การทำ Computer Forensics คือขั้นตอนการพิสูจน์หลักฐานทางคอมพิวเตอร์ ที่จะต้องเผชิญกับเหตุการการตรวจสอบข้อมูลต่างๆทาง

คอมพิวเตอร์ที่เกิดขึ้นในโลกไซเบอร์ใบนี้ และเหตุการ ณ์บางอย่างที่เกิดขึ้น ไม่ได้มีการเตรียมตัวมาก่อน ที่จะจัดการกับเหตุการณ์ที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ

โดยทั่วไปในองค์กรจะมีการรักษาความปลอดภัยด้วยการใช้ไฟร์วอล และอัพเดตโปรแกรมป้องกันไวรัส อย่างไรก็ตามองค์กรส่วนใหญ่ไม่ได้มีนโยบายควบคุมการใช้อุปกรณ์ USB ซึ่งทำให้สามารถใช้อุปกรณ์นี้เชื่อมต่อกับระบบเครือข่ายและระบบโทรศัพท์ได้ ซึ่งอาจทำให้เกิดการรับส่งข้อมูล ขององค์กร และเมื่อมีการยกเลิกสัญญาพนักงาน จึงต้องมีการปิดบัญชีผู้ใช้ให้ทันท่วงที

องค์กรทั่วไปจะมีกฎและข้อบังคับเกี่ยวกับการรักษาข้อมูลลูกค้า อย่างไรก็ตามการรั่วไหลของข้อมูลยังคงเป็นปัญหาใหญ่ที่องค์กรเหล่านี้ต้องเผชิญอยู่ในโลกของเทคโนโลยีทุกวันนี้

เมื่อมีเหตุการเกิดขึ้นกับคอมพิวเตอร์แน่นอนว่าในที่สุด ทุกองค์กรจะต้องมีการจัดการกับเหตุการที่เกิดขึ้นในโลกไซเบอร์ ตัวอย่างของเหตุการในโลกไซเบอร์ที่พบกันบ่อย ๆซึ่งอาชญกรรมที่พบบ่อยได้แก่

- การทุจริตทางคอมพิวเตอร์
- อาชญกรรม
- การจารกรรมข้อมูลในภาคอุตสหกรรม
- การโจรกรรมข้อมูลลับขององค์กร
- การละเมิดลิขสิทธ์ส่วนบุคคล / การสูญเสียข้อมูลของลูกค้า
- สือลามกอนาจารสำหรับเด็กและผู้ใหญ่
- การกระทำต่างๆที่เป็นการละเมิดนโยบายการรักษาความปลอดภัยของคอมพิวเตอร์ขององค์กร และอื่น ๆ

เมื่อมีเหตุการณ์ดังกล่าวเกิดขึ้นผู้กระทำผิดจะทิ้งช่องโหว่ เช่น ทาง จริยธรรม ทางการเงิน และถูกทาง กฎหมาย เหตุการณ์ที่เกิดขึ้นต้องได้รับการตรวจสอบอย่างจริงจัง โดยเริ่มจาก การตรวจสอบหลักฐานจากภายใน อย่างรวดเร็วเพื่อขยายผลไปสู่การตรวจสอบคดีทางอาญาซึ่งจะเกี่ยวข้องกับหน่วยงานภายนอกโดยข้อมูลการสอบสวนอาจรั่วไหลสู่ภายนอกโดยไม่รู้ตัว

จากการสำรวจคดีสำคัญทางอาชญกรรมทางเศรษฐกิจทั่วโลก ในปี 2011

- ในขณะนี้อาชญกรรมทางคอมพิวเตอร์จัดเป็นหนึ่งในสี่ของอาชญกรรมทางเศรษฐกิจที่สำคัญ
- 40 % ของผู้ตอบแบบสอบถามหวาดกลัวในเรื่องของภาพลักษ์ชื่อเสียงขององค์กรมากที่สุด
- 60% กล่าวว่า องค์กรไม่มีนโยบายติดตามความเคลื่อนไหวในสื่อสังคมออนไลน์
- 34% ของผู้ตอบแบบสอบถามมีประสบการณ์ที่เกี่ยวข้องกับอาชญกรรมทางเศรษฐกิจในช่วง 12 เดือนที่ผ่านมา (เพิ่มขึ้น 30 % จากปี 2009)
- เกือบ 1 ใน 10 ที่เปิดเผยถึงความเสียหายจากอาชญกรรมทางเศรษฐกิจมากกว่า 5 หมื่นล้านเหรียญสหรัฐ

- 56 % ของผู้ตอบแบบสอบถามกล่าวว่าการทุจริตที่ร้ายแรงที่สุดคือ “ภายในองค์กรนั่นเอง”
- 2 ใน 5 ของผู้ตอบแบบสอบถามไม่ได้รับการฝึกอบรมใดๆเลยเกี่ยวกับความปลอดภัย ในโลกไซเบอร์
- ผู้ตอบแบบสอบถามส่วนใหญ่ไม่ได้ตระหนักถึงการมีแผนรองรับหรือรับมือในกรณีถ้ามีอาชญกรรมทางคอมพิวเตอร์เกิดขึ้นภายในองค์กร

ทำไม การทำ Computer Forensics จึงมีความสำคัญต่อองค์กรคุณ

เมื่อองค์กรต้องเผชิญกับเหตุการณ์ในระบบรักษาความปลอดภัยขององค์กร ส่วนใหญ่เจ้าหน้า ที่ทางไอทีจะถูกคาดหวังในประเมินปัญหาที่เกิดขึ้นในเบื้องต้นและพยายามหาข้อเท็จจริงของเหตุการที่เกิดขึ้นและ ประเมินระดับของความรุนแรง ส่วนใหญ่พนักงานไอทีในบรัษัททั่วไปไม่ได้รับการฝึกอบรมในด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์(Computer Forensic) ส่งผลให้พวกเขาไม่ตระหนักถึงวิธีการเก็บข้อมูลหลักฐานทางดิจิตอลหรือคอมพิวเตอร์ที่อาจจะต้องนำไปเป็นหลักฐานแสดงต่อศาลในกรณีที่มีการร้องขอ ข้อมูลที่สำคัญอย่างเช่น วันและเวลาที่ปรากฏ อาจสูญหายหรือเปลี่ยนแปลง ซึ่งจะทำให้การตรวจสอบยากมากขึ้น ในสถานการณ์ที่เลยร้ายที่สุดข้อมูลที่ตรวจพบอาจไม่เป็นที่ยอมรับเมื่อนำไปเสนอในชั้นศาล

การพิสูจน์หลักฐานทางคอมพิวเตอร์จำเป็นต้องมีทักษะเฉพาะซึ่งเกี่ยวข้องกับการเก็บรักษาข้อมูลและตรวจสอบ แยกแยะหลักฐานทางคอมพิวเตอร์ที่พบ แต่การ เผยแพร่หลักฐานที่ถูกต้อง เมื่อต้องเผชิญหลักฐานทางคอมพิวเตอร์องค์กรมีแนวโน้มที่จะเน้นไปที่ค่าใช้ จ่ายที่เกี่ยวข้อง และขึ้นอยู่กั บความซับซ้อนของการ

ตรวจสอบข้อมูลหลักฐานและจำนวนเครื่องคอมพิวเตอร์ที่เกี่ยวข้อง แต่อย่างไรก็ตามค่าใช้จ่ายจะขึ้นอยู่กับสิ่งต่อไปนี้

- หลักฐานที่ได้จากการตรวจสอบหลักฐานทางคอมพิวเตอร์ จะเป็นผลลัพธ์ของการสืบสวน
- การพิสูจน์หลักฐานทางคอมพิวเตอร์สามารถลดขั้นตอนการดำเนินการทางกฎหมายให้รวดเร็วกระชับขึ้น
- การพิสูจน์หลักฐานทางคอมพิวเตอร์ สามารถประหยัดเวลาในการตรวจสอบซึ่งยังสามารถช่วยองค์กรประหยัดค่าใช้จ่ายด้วย

เมื่อองค์กรกำหนดแผนรับมือกับเหตุการณ์ที่อาจจะเกิดขึ้น องค์กรควรจะสร้างแผนการซึ่งตอบสนองงานด้านพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ซึ่งอาจหมายถึง การให้พนักงานได้รับการอบรมการเก็บ ตรวจสอบ พิสูจน์หลักฐานทางคอมพิวเตอร์ที่ถูกต้องตามหลักสากลในองค์กร ซึ่งพนักงานที่ผ่านการฝึกอบรมสามารถช่วยเหลือองค์กรเบื้องต้นในกรณีเกิดอาชญกรรมทางคอมพิวเตอร์

การพิสูจน์หลักฐานทางคอมพิวเตอร์เริ่มเป็นที่สนใจในหลายๆประเทศทั่วโลก ปัจจุบันนี้ในประเทศ อังกฤษได้ก่อตั้งโครงการ Insurance Scheme ซึ่งเป็นองค์กรที่ให้ความช่วยเหลือลูกค้าถ้ามีการเรียกร้องการตรวจสอบพิสูจน์หลักฐานทางคอมพิวเตอร์ โดยองค์กรต้องยอมรับการพิสู จน์หลักฐานทางคอมพิวเตอร์และเป็นเครื่องมือในการควบคุมผู้ที่กำลังคิดที่จะก่ออาชญกรรมทางคอมพิวเตอร์