SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 2 ฉบับที่ 17 ประจำเดือน ธันวาคม 2553

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

จดหมายข่าวฉบับนี้นำเสนอมุมมองใหม่ด้านการรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้ง ครอบคลุมเรื่องการให้บริการประเมินความเสี่ยงระบบสารสนเทศในรูปแบบ SaaS และจัดเปรียบเทียบให้สอดคล้องตามมาตรฐาน PCI DSS...ติดตามอ่านได้ในฉบับค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- จุดเปลี่ยนสู่การรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้ง หน้า 1-5
- Message from SRAN หน้า 1
- มารู้จักมาตรฐาน PCI DSS หน้า 5

Message from SRAN

SRAN Light : Firmware version วันที่ 23 พฤศจิกายน 2553

Changelog

- Add snmp option to get MAC address from Switch.

SRAN Security Center : Firmware version วันที่ 23 พฤศจิกายน 2553

Changelog

- Update hybrid archive page

จุดเปลี่ยน สู่การรักษาความปลอดภัยไอที ผ่าน 'ระบบคลาวด์คอมพิวติ้ง'

ทำอย่างไรองค์กรจึงจะบริหารจัดการความเสี่ยงด้านไอทีโดยใช้คนและงบประมาณน้อยที่สุด?

มักมีคำถามว่า องค์กรขนาดกลางและขนาดเล็กจะสามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้เป็นไปตามมาตรฐานและกฎระเบียบความปลอดภัยได้อย่างไร โดยใช้บุคคลากรและงบประมาณการลงทุนที่มีอยู่จำกัด

การที่จะทำให้ระบบเทคโนโลยีสารสนเทศเป็นไปตามมาตรฐานความปลอดภัยด้านต่างๆ โดยเฉพาะกับองค์กรขนาดกลางและขนาดเล็กนั้น อาจดูเป็นเรื่องไกลตัว ยากจะบริหารจัดการได้ ด้วยสาเหตุนานาประการ แต่แนวโน้มทางเทคโนโลยีในปัจจุบันได้แสดงให้เห็นว่าเป็นสิ่งที่เป็นไปได้และไม่ควรมองข้าม เนื่องจากประเด็นดังต่อไปนี้ ...

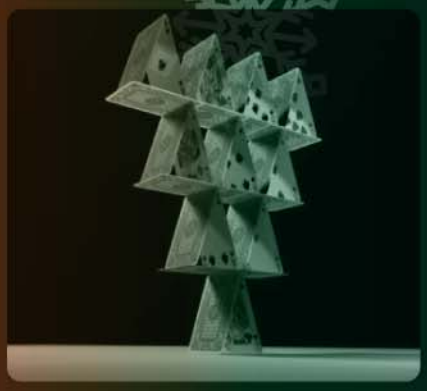
อ่านต่อหน้า 2

กำหนดการฝึกอบรมการใช้งาน SRAN **ฟรี!** สำหรับลูกค้าและตัวแทนจำหน่าย ประจำปี 2553-2554

ธ.ค. 2010	2011	ม.ค.	ก.พ.	มี.ค.	พ.ค.	ก.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
23-24	Red Course / SRAN Security Center (สำหรับลูกค้า)	19	16	16	20	18	15	20	17	21	19	16	14
	Red Course / SRAN Light (สำหรับลูกค้า)	20	17	17	21	19	16	21	18	22	20	17	14

จุดเปลี่ยนสู่การรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้ง

การที่จะทำให้ระบบเทคโนโลยีสารสนเทศเป็นไปตามมาตรฐานความปลอดภัยด้านต่างๆ โดยเฉพาะกับองค์กรขนาดกลางและขนาดเล็กนั้นอาจดูเป็นเรื่องไกลตัวยากจะบริหารจัดการได้ ด้วยสาเหตุนานาประการ แต่แนวโน้มทางเทคโนโลยีในปัจจุบันได้แสดงให้เห็นว่าเป็นสิ่งที่เป็นไปได้และไม่ควรมองข้าม เนื่องจากประเด็นดังต่อไปนี้



1. การคุกคามในโลกไซเบอร์และกฎเกณฑ์ที่ใช้ควบคุมไม่ได้ขึ้นอยู่กับขนาดของธุรกิจ

ผู้คุกคาม (attacker) มิได้สนใจว่าเป้าหมายของตนจะเป็นบริษัทฯ ชั้นนำหรือเป็นเพียงบริษัทฯ ขนาดเล็กที่ไม่มีชื่อเสียง แต่สิ่งที่หน่วยงานด้านกฎหมายมองเห็นคือไม่ว่าจะเป็นองค์กรขนาดใดก็ตาม หลักเกณฑ์เรื่องความปลอดภัยก็ไม่ควรที่จะแตกต่างกัน ดูได้จากกฎหมายที่ควบคุมเกี่ยวกับสิทธิส่วนบุคคลก็มิได้ระบุว่าแต่ละบุคคลแตกต่างกัน แต่กรณีที่เกิดภัย คุกคามขึ้นนั้น โทษจะต่างกันไปตามมูลค่าหรือปริมาณความเสียหายที่เกิดขึ้น ไม่เหมือนกับการปฏิบัติตามมาตรฐาน เช่น HIPAA, PCI DSS หรือมาตรฐานอื่นๆ ที่ค่อนข้างเฉพาะเจาะจงกับผู้ให้บริการให้ธุรกิจนั้นๆ ซึ่งจะส่งผลกระทบต่อองค์กรขนาดกลางและขนาดเล็กด้วย โดยมิได้ขึ้นอยู่กับขนาดขององค์กร

2. ข้อบกพร่องและช่องโหว่ของซอฟต์แวร์...ประเด็นที่พึงตระหนักมากขึ้น

ปริมาณช่องโหว่ซอฟต์แวร์ที่ประกาศออกมาสู่สาธารณชนมีปริมาณเพิ่มมากขึ้นทุกวัน อ้างอิงตามรายละเอียดภัยคุกคามซึ่งเปิดเผยสู่สาธารณชนทั่วไปซึ่งจัดทำโดยศูนย์ความปลอดภัยทางไซเบอร์แห่งชาติประเทศสหรัฐอเมริกา รายงานว่ามีช่องโหว่มากกว่า 3,500 รายการได้ถูกตรวจพบในช่วง 3 ไตรมาสแรกของปี 2010 ซึ่งหมายถึงมีช่องโหว่ใหม่ๆ เพิ่มขึ้น 10 รายการ ในทุกๆ วัน และช่องโหว่หรือข้อบกพร่องเหล่านี้เป็นช่องทางที่นักจู่โจมและมัลแวร์สามารถเข้าถึงระบบที่ได้ถูกป้องกันไว้เป็นอย่างดี เหตุการณ์ลักษณะนี้มีโอกาสเกิดขึ้นเท่าๆ กัน ไม่ว่าองค์กรธุรกิจของคุณจะเล็กหรือใหญ่ สิ่งเหล่านี้มิใช่จะเกิดความเสี่ยงขึ้นกับระบบปฏิบัติการ เครื่องคอมพิวเตอร์แม่ข่าย และซอฟต์แวร์ที่ติดตั้งใช้งานอยู่เท่านั้น หากยังรวมถึงเว็บแอพพลิเคชั่นด้วยเช่นกัน และจากการศึกษาเมื่อเร็วๆ นี้พบว่าโดเมนเว็บมากกว่าล้านแห่ง ติดมัลแวร์ภายใน 90 วัน ภายหลังจากการเปิดให้บริการ

3. การเพิ่มขึ้นของความเสี่ยงในการดำเนินธุรกิจ อันเนื่องมาจากคู่ค้า ผู้ขาย และ ผู้มีส่วนได้ส่วนเสียในการดำเนินธุรกิจ

ธุรกิจส่วนใหญ่อยู่ภายใต้แรงกดดันทั้งจากภายในและภายนอกองค์กร องค์กรธุรกิจส่วนใหญ่ต้องการจะมีแผนงานด้านความปลอดภัยและการบริหารความเสี่ยงในการดำเนินธุรกิจ ต้องการแผนการกู้คืนระบบและขั้นตอนที่ทำให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง ต้องการทราบถึงกรรมวิธีในการป้องกันและบริหารจัดการทางด้านความปลอดภัย ทั้งยังต้องการทราบว่าข้อมูลที่เป็นความลับของตนได้รับการดูแลปกป้องอย่างไร ในขณะที่กฎหมายที่เกี่ยวข้องทางด้านความปลอดภัย และมาตรฐานทางด้านความปลอดภัยนั้น มักส่งผลกระทบต่อองค์กรขนาดเล็กและขนาดกลางซึ่งขาดบุคลากรที่มีประสบการณ์หรือเงินลงทุนที่จะต่อสู้กับภัยคุกคามและรักษาไว้ซึ่งมาตรฐานและกฎเกณฑ์ต่างๆ ขององค์กร จากผลการสำรวจหลายแห่งพบว่าองค์กรขนาดกลางและขนาดเล็กใช้เวลากว่า 2 ใน 3 กับการบริหารจัดการด้านไอที และงบประมาณปีละกว่า 51,000 เหรียญสหรัฐในการให้ความสำคัญกับเรื่องของความปลอดภัยข้อมูลสารสนเทศ ถือเป็นระยะเวลามากกว่า 2 เท่า และใช้เงินงบประมาณมากขึ้น 27.5% เมื่อเทียบกับการลงทุนเกี่ยวกับคอมพิวเตอร์ในด้านอื่นๆ จึงนับเป็นมูลค่าการลงทุนด้านความปลอดภัยที่สูงเอาการทีเดียว

จุดเปลี่ยนสู่การรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้ง

ลูกค้าส่วนใหญ่มักเคยประสบปัญหารูปแบบเดียวกัน ว่าความพยายามให้ระบบข้อมูลสารสนเทศมีความมั่นคงปลอดภัยนั้น ต้องแลกกับเวลามากมายที่สูญไปกับการติดตั้ง การบำรุงรักษา การบริหารจัดการทั้งในส่วนของซอฟต์แวร์และฮาร์ด-แวร์ รวมทั้งต้นทุนทั้งในแง่ของเม็ดเงินและบุคลากร ด้วยเหตุนี้หลายองค์กรจึงพยายามที่จะเปลี่ยนไปใช้ซอฟต์แวร์โอเพ่นซอร์ส หรือเลือกใช้ซอฟต์แวร์ราคาถูกที่หาได้โดยง่ายในท้องตลาดทั่วไป สิ่งเหล่านี้จะช่วยประหยัดงบ-ประมาณได้เพียงบางส่วนในช่วงเริ่ม-ต้นเท่านั้น หากแต่ไม่สามารถลดต้นทุนได้อย่างแท้จริง เนื่องจากค่าใช้จ่ายด้านซอฟต์แวร์มิได้เป็นต้นทุนระยะยาว ต้นทุนหลักที่มีมูลค่าสูงลิ่วคือต้นทุนด้านแรงงาน การสร้างและบำรุงรักษาโครงสร้างพื้นฐาน การปรับปรุงและตั้งค่าของแอพพลิเคชั่นที่เหมาะสมต่างหาก

ผลท้ายที่สุดคือคว้าน้ำเหลว ไม่สามารถบริหารจัดการความปลอดภัยไอทีได้อย่างมีประสิทธิภาพ เครื่องมือที่นำมาใช้กลับยากต่อการบริหารจัดการ ต้องการทีมผู้เชี่ยวชาญเฉพาะด้านมาทุ่มเทดูแลระบบ และรายงานที่ได้ไม่สอดรับกับความเป็นจริงและให้ผลลัพธ์ที่ไม่ถูกต้องบ่อยครั้ง ไม่อาจบรรลุเป้าหมายด้านความปลอดภัยและการปฏิบัติให้สอดคล้องตามมาตรฐานได้ อีกทั้งระบบซอฟต์แวร์ก็เป็นภาระในการดูแลรักษาและมักจะมีปัญหาเมื่อเรียกใช้งาน ในที่สุดเครื่องมือที่ยุ่งยากนี้ก็จะเสียเปล่า ไม่ได้ใช้ประโยชน์ ผลที่ตามมาก็คือไม่มีการประเมินความเสี่ยงและแก้ไขปัญหาที่เกิดขึ้น ไม่มีการปรับปรุงเงื่อนไขการตั้งค่าไฟร์วอลล์ให้ทันสมัย และ ช่องโหว่ของเว็บเซิร์ฟเวอร์ก็สะสมเป็นดินพอกหางหมู สุดท้ายระบบไอทีขององค์กรก็ไร้ความปลอดภัย โอกาสที่ภัย-คุกคามหรือผู้ไม่ประสงค์ดีจะโจมตีได้สำเร็จก็เพิ่มมากขึ้น และองค์กรก็ไม่อาจบรรลุเกณฑ์ประเมินด้านมาตรฐานความปลอดภัยได้

จุดเปลี่ยนสู่ความปลอดภัยบนเครือข่ายคลาวด์คอมพิวติ้ง

ความต้องการหลีกเลี่ยงปัญหาด้านต้นทุนและความซับซ้อนของระบบซอฟต์แวร์ เป็นเหตุผลสำคัญให้องค์กรส่วนใหญ่ลงทุนในโซลูชั่นคลาวด์ และ Software-as-a-service (SaaS) ซึ่งมีข้อได้เปรียบหลักด้านต้นทุนที่ต่ำกว่า ใช้ระยะเวลาน้อย มีความยืดหยุ่นสูง และที่สำคัญคือจ่ายเท่าที่ใช้เท่านั้น ตัวอย่างที่เห็นได้ง่ายคือ เมื่อมีการปรับปรุงรุ่นของซอฟต์แวร์ หากเป็นแบบเดิมจะต้องทำการปรับปรุงรุ่นให้ลูกค้าแต่ละรายเป็นการเฉพาะ เนื่องจากลูกค้าแต่ละรายมีความต้องการแตกต่างกัน แต่หากเป็นบริการแบบ SaaS การปรับปรุงรุ่นของซอฟต์แวร์กระทำจากที่เดียวครั้งเดียว แล้วลูกค้าทุกรายก็จะได้ใช้ซอฟต์แวร์ใหม่ๆ แบบเดียวกันในทุกองค์กร โดยไม่มีปัญหาเรื่องการตั้งค่าซอฟต์แวร์ไม่ถูกต้อง ด้วยเหตุนี้ภาระหน้าที่ในการดูแลรักษาแอพพลิเคชั่นด้านความ-ปลอดภัยจึงถูกเปลี่ยนมือไปสู่ผู้ให้บริการด้านซอฟต์แวร์ (Software Service Provider) แทนที่จะเป็นบุคลากรภายในองค์กร

ประโยชน์ที่องค์กรจะได้รับคือต้นทุนและความซับซ้อนในการบริหารจัดการที่ลดลง ตลอดจนลดปัญหาด้านการสรรหาบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน ด้วยเหตุนี้แอพพลิเคชั่นด้านความปลอดภัยและการบริหารจัดการความเสี่ยงทางธุรกิจจึงมุ่งไปสู่ระบบคลาวด์ ไม่ว่าจะเป็นการบริหารจัดการเกี่ยวกับอีเมล์ (E-mail Management) ระบบการกรองเนื้อหาข้อมูล (Content Filtering) ระบบการกู้คืนข้อมูลหลังเกิดภัยพิบัติเพื่อให้ธุรกิจสามารถดำเนินต่อไปได้อย่างต่อเนื่อง (Disaster-Recovery/Business Continuity) การบริหารจัดการด้านการประเมินความเสี่ยง (Vulnerability Management) ตลอดจนเทคโนโลยีอื่นๆ อีกหลายรูปแบบ

จุดเปลี่ยนสู่การรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้ง

กุญแจสำคัญที่เป็นลักษณะเฉพาะของการรักษาความปลอดภัยไอทีบนระบบคลาวด์นั้น คือการที่ไม่ต้องติดตั้งอุปกรณ์หรือซอฟต์แวร์ในองค์กรของผู้ใช้บริการ เนื่องจากผู้ให้บริการ SaaS จะเป็นผู้จัดหาพร้อมติดตั้งอุปกรณ์ที่จำเป็นต่อการใช้งานไว้ ให้ใช้งาน ณ ศูนย์ข้อมูลที่มีการรักษาความปลอดภัยเป็นอย่างดี ประเด็นสำคัญอีกประการหนึ่งคือการประหยัดต้นทุน ส่งผลให้องค์กรธุรกิจสามารถควบคุมค่าใช้จ่ายได้อย่างมีประสิทธิภาพ

ประโยชน์ที่องค์กรขนาดกลางและขนาดเล็ก จะได้รับจากบริการรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้งและ SaaS

1. มีการใช้ฮาร์ดแวร์เท่าที่จำเป็น เพราะแทบไม่จำเป็นต้องใช้อุปกรณ์ในสำนักงานของผู้ใช้บริการเลย
2. ใช้งานได้อย่างต่อเนื่อง เนื่องจากระบบคลาวด์คอมพิวติ้งสามารถเรียกใช้งานได้ตลอดเวลา โดยใช้เว็บไซต์เป็นกลไกในการเคลื่อนย้ายข้อมูลไปสู่ศูนย์ข้อมูลของผู้ใช้บริการ นอกจากนี้ผู้ใช้บริการยังจะได้รับการปรับปรุงรุ่นและบริการต่างๆ จากผู้ให้บริการโดยอัตโนมัติ หรือเมื่อได้รับการร้องขอ
3. จ่ายเท่าที่ใช้งานเท่านั้น แอพพลิเคชั่นบนระบบคลาวด์จะประมวลผลก็ต่อเมื่อได้รับคำสั่งหรือได้รับการร้องขอ ดังนั้นผู้ใช้บริการจึงสามารถควบคุมค่าใช้จ่ายได้ด้วยโมเดลการจ่ายเงินเท่าที่ใช้งาน
4. มีข้อมูลภัยคุกคามที่ทันสมัยที่สุดตลอดเวลา การทราบถึงข้อมูลความเสี่ยง ภัยคุกคาม โปรแกรมร้ายแรง ตลอดจนเว็บไซต์หลอกลวงนั้น ต้องอาศัยทีมวิจัยที่มีความเชี่ยวชาญเฉพาะด้านในการค้นหาข้อมูลรูปแบบของภัยคุกคาม และปรับปรุงกรรมวิธีในการตรวจสอบความปลอดภัยด้านต่างๆ ระบบคลาวด์จะช่วยให้มั่นใจได้ว่ามีข้อมูลภัยคุกคามที่ทันสมัยที่สุดทุกครั้งที่องค์กรเข้าใช้บริการ

Qualys ถือเป็นตัวอย่างหนึ่งของการใช้รูปแบบของคลาวด์คอมพิวติ้งมาให้บริการในโซลูชั่นด้านการประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศและการรับรองมาตรฐาน ช่วยเพิ่มความปลอดภัยให้กับองค์กรทุกขนาดทั้งในระดับเครือข่ายและแอพพลิเคชั่น ตลอดจนทำการตรวจประเมินความปลอดภัยระบบสารสนเทศโดยอัตโนมัติเพื่อให้สอดคล้องกับหลักเกณฑ์มาตรฐานที่กำหนดไว้

หนึ่งในการให้บริการในรูปแบบ SaaS คือบริการ QualysGuard ซึ่งสามารถใช้งานได้ทันทีภายในเวลาไม่กี่ชั่วโมง ไม่ว่าจะอยู่ ณ ที่ใดในโลกก็จะได้รับข้อมูลด้านความปลอดภัยและการรับรองมาตรฐานโดยทันที ด้วยเหตุนี้ QualysGuard จึงเป็นโซลูชั่นที่ได้รับการยอมรับและใช้งานอย่างแพร่หลายไปทั่วโลก ครอบคลุมบริการบริหารจัดการและประเมินความเสี่ยงข้อมูลสารสนเทศ การสแกนเว็บแอพพลิเคชั่นและบริการตรวจหามัลแวร์ ช่วยให้ตรวจพบช่องโหว่ในระบบสารสนเทศและแก้ไขได้อย่างทันท่วงที

จุดเปลี่ยนสู่การรักษาความปลอดภัยไอทีผ่านระบบคลาวด์คอมพิวติ้ง

มารู้จักมาตรฐาน PCI DSS

มาตรฐาน PCI DSS ย่อมาจาก "Payment Card Industry Data Security Standard" เป็นมาตรฐานความปลอดภัยสารสนเทศที่แพร่หลายทั่วโลก ถูกกำหนดขึ้นเพื่อช่วยให้องค์กรต่างๆ ที่มีการรับชำระเงินด้วยบัตรเครดิต สามารถป้องกันการฉ้อโกงบัตรเครดิต โดยการควบคุมข้อมูลและช่องโหว่ต่างๆ ให้เข้มงวดมากยิ่งขึ้น และได้นำไปใช้กับทุกองค์กรที่เก็บรักษา ประมวลผล หรือรับส่งข้อมูลของผู้ถือบัตรเครดิต ไม่ว่าจะเป็นบัตรของค่ายใดก็ตาม

การตรวจสอบการปฏิบัติตามมาตรฐานอาจทำได้โดยตรวจสอบเองด้วยบุคลากรภายในองค์กรหรือให้หน่วยงานภายนอกเป็นผู้ตรวจสอบก็ได้ ซึ่งจะใช้วิธีใดไม่เกี่ยวกับขนาดองค์กร แต่ขึ้นกับปริมาณการทำธุรกรรมผ่านบัตรเครดิตขององค์กรนั้นๆ การประเมินการปฏิบัติตามมาตรฐาน PCI DSS จะต้องทำเป็นประจำทุกปี โดยองค์กรที่มีปริมาณธุรกรรมผ่านบัตรเครดิตมากจะต้องได้รับการตรวจประเมินจากผู้ตรวจประเมินอิสระ (Qualified Security Assessor : QSA) ส่วนบริษัทที่มีปริมาณธุรกรรมไม่มากนัก สามารถเลือกที่จะตรวจประเมินได้ด้วยตนเองผ่านแบบสำรวจประเมินตนเอง (Self-Assessment Questionnaire : SAQ)

เนื่องจากมาตรฐาน PCI DSS ส่งกระทบต่อเครือข่ายและงานด้านสารสนเทศของทุกองค์กรที่เก็บข้อมูล ประมวลผล และส่งต่อข้อมูลของผู้ถือบัตร การตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายสารสนเทศ จึงเป็นสิ่งจำเป็นต่อการปกป้องข้อมูลของผู้ถือบัตร หากองค์กรใดไม่เคยตรวจสอบระบบของตนเลย ก็ทำได้เพียงตั้งความหวังว่าข้อมูลของผู้ถือบัตรจะอยู่รอดปลอดภัยเท่านั้น

ด้วยเหตุนี้ การประเมินความเสี่ยงเพื่อตรวจหาช่องโหว่ (Vulnerability Assessment) จึงเป็นวิธีเดียวที่ช่วยวัดระดับความปลอดภัย และยกระดับความคุ้มครองให้สูงสุด ทั้งยังสอดคล้องตามมาตรฐาน PCI DSS อีกด้วย ซึ่งการประเมินความเสี่ยงให้สอดคล้องกับ PCI DSS นั้นจะต้องสแกนหาช่องโหว่ทั้งภายในและภายนอกเครือข่ายเป็นประจำอย่างต่อเนื่อง เพื่อตรวจหาช่องโหว่ใหม่ๆ และปิดช่องโหว่ดังกล่าว โดยเฉพาะเมื่อมีการ เปลี่ยนแปลงเครือข่ายครั้งสำคัญ เช่น ติดตั้งระบบใหม่, เปลี่ยนโครงสร้างเครือข่าย, ปรับค่าไฟร์วอลล์ เป็นต้น

แน่นอนว่าการมีเครื่องมือที่ดีและทรงประสิทธิภาพอย่างไรก็ไม่เกิดผล หากปราศจากทีมงานมืออาชีพที่มีความเชี่ยวชาญเฉพาะด้าน และสื่อสารด้วยภาษาเดียวกัน บริษัทโกลบอลเทคโนโลยีฯ จึงผนึกกำลังกับ Qualys ในการให้บริการประเมินความเสี่ยงระบบสารสนเทศในรูปแบบ SaaS และจัดเปรียบเทียบให้สอดคล้องตามมาตรฐาน PCI DSS ตลอดจนการให้คำปรึกษา และแก้ไขปัญหาที่เกี่ยวข้องกับความปลอดภัยข้อมูลสารสนเทศ

สอบถามรายละเอียดเพิ่มเติมเกี่ยวกับผลิตภัณฑ์และบริการของบริษัทได้ที่

info@gbtech.co.th
หรือโทร. 02-982-5445

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