ความแตกต่างของความปลอดภัยบนคลาวด์

บทความโดยเร้ดแฮท

การรักษาความปลอดภัยให้กับระบบคลาวด์ คือการปกป้องข้อมูล ปกป้องแอปพลิเคชั่น และปกป้องโครงสร้างพื้นฐานที่เกี่ยวข้องกับระบบคลาวด์คอมพิวติ้งทั้งหมด ซึ่งลักษณะหลายประการของความปลอดภัยบนสภาพแวดล้อมคลาวด์ (ไม่ว่าจะเป็นพับลิค ไพรเวท หรือไฮบริดคลาวด์) ก็เหมือนกับการรักษาความปลอดภัยของระบบไอทีที่ติดตั้งในองค์กร

ความกังวลด้านการรักษาความปลอดภัยระดับสูง เช่น การเปิดเผยข้อมูลที่ไม่ได้รับอนุญาตและการรั่วไหลของข้อมูล การควบคุมการเข้าถึงข้อมูลที่ไม่เข้มงวดพอ ความไวของระบบต่อการถูกโจมตี และความพร้อมใช้งานที่ต้องหยุดชะงักลง ซึ่งส่งผลกระทบต่อระบบไอทีแบบดั้งเดิมและระบบคลาวด์เหมือนกัน ระบบคลาวด์จึงต้องมีการป้องกันและรักษาความปลอดภัยให้มากเพียงพอ เช่นเดียวกันกับสภาพแวดล้อมด้านคอมพิวติ้งอื่น ๆ ดังนั้นองค์กรต่าง ๆ จะต้องมีความสามารถดังต่อไปนี้

- ทราบว่าข้อมูลและระบบมีความปลอดภัย

- สามารถมองเห็นและรับรู้ถึงสถานะของการรักษาความปลอดภัยที่เป็นอยู่ในปัจจุบัน
- รู้ถึงความผิดปกติขึ้นในระบบได้อย่างทันที
- สามารถติดตามและตอบสนองต่อเหตุการณ์ที่ไม่คาดคิดได้อย่างทันท่วงที

ทำไมการรักษาความปลอดภัยบนคลาวด์จึงแตกต่างกัน

ในขณะที่หลาย ๆ คนเข้าใจถึงประโยชน์ของคลาวด์คอมพิวติ้ง แต่ในขณะเดียวกันพวกเขาก็มีความกังวลเกี่ยวกับภัยคุกคามด้านความปลอดภัยเช่นกัน ซึ่งเป็นที่เข้าใจได้ เพราะมันเป็นเรื่องที่จะต้องอธิบายให้เห็นภาพของสิ่งที่เป็นนามธรรมจับต้องไม่ได้ ที่ถูกส่งผ่านระหว่างอินเทอร์เน็ตและเครื่องเซิร์ฟเวอร์ ซึ่งเป็นสภาพแวดล้อมที่ไดนามิกที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา เช่นเรื่องของภัยคุกคาม แต่สิ่งสำคัญคือในหลายส่วนความปลอดภัยของคลาวด์ก็คือความปลอดภัยของระบบไอที ซึ่งเมื่อเข้าใจความแตกต่างที่เฉพาะเจาะจงแล้วก็จะไม่รู้สึกว่า “คลาวด์” ไม่ปลอดภัยอีกต่อไป

ขอบเขตความปลอดภัยไม่มีที่สิ้นสุด

การรักษาความปลอดภัยเกี่ยวข้องกับความสามารถในการเข้าถึงข้อมูลเป็นอย่างมาก สภาพแวดล้อมแบบดั้งเดิมมักควบคุมการเข้าถึงโดยการใช้โมเดล perimeter security แต่สภาพแวดล้อมคลาวด์มีการเชื่อมต่อกันมากทำให้ทราฟฟิกในการรับส่งข้อมูลสามารถหลีกเลี่ยงการรักษาความปลอดภัยในแบบของระบบดั้งเดิมได้ง่าย อินเทอร์เฟซช่องทางการเชื่อมต่อการทำงาน (Application Programming Interfaces: APIs) ที่ไม่ปลอดภัย การจัดการข้อมูลส่วนบุคคลและข้อมูลในการระบุตัวตนที่ไม่รัดกุม การขโมยข้อมูลทางบัญชี และบุคคลภายในองค์กรที่มีเจตนาร้าย อาจเป็นภัยคุกคามต่อระบบและข้อมูลได้ การป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตบนระบบคลาวด์นั้น จำเป็นต้องใช้วิธีที่ให้ข้อมูลเป็นศูนย์กลาง (data-centric) การเข้ารหัสข้อมูล การทำให้กระบวนการอนุมัติรัดกุมมากขึ้น ต้องมีรหัสผ่านที่แน่นหนา และการยืนยันตัวตนที่จะต้องให้ผู้ใช้งานใส่รหัสอีกหนึ่งชุดนอกเหนือจากรหัสผ่านส่วนตัวของเขา ซึ่งเป็นการสร้างความปลอดภัยให้กับทุกระดับการใช้งาน

สิ่งจำเป็นทุกอย่างมีอยู่ในซอฟต์แวร์

“คลาวด์” คือการส่งมอบทรัพยากรด้านไอทีที่โฮสต์ไว้ไปยังผู้ใช้งานผ่านซอฟต์แวร์ โครงสร้างพื้นฐานคลาวด์คอมพิวติ้งพร้อมด้วยข้อมูลต่าง ๆ ที่กำลังประมวลผลนั้นมีความเคลื่อนไหวอยู่ตลอดเวลา สามารถปรับขยายและเคลื่อนย้ายได้ การควบคุมความปลอดภัยบนคลาวด์จำเป็นต้องสนองตอบต่อตัวแปรที่อยู่ในสภาพแวดล้อมต่าง ๆ ควบคู่กับเวิร์กโหลดและข้อมูลที่ไม่ได้ใช้งานและที่อยู่ระหว่างดำเนินงาน ไม่ว่าจะเป็นส่วนหนึ่งของเวิร์กโหลด (เช่น การเข้ารหัส) หรือเคลื่อนไหวผ่านระบบการจัดการคลาวด์และ APIs ซึ่งเป็นการช่วยปกป้องสภาพแวดล้อมคลาวด์จากความเสียหายของระบบและจากการสูญหายของข้อมูลได้

ภัยคุกคามที่มีความเสี่ยงสูง

ภัยคุกคามที่มีความเสี่ยงสูง คืออะไรก็ตามที่ส่งผลกระทบเชิงลบต่อระบบคอมพิวเตอร์รุ่นใหม่ ๆ ซึ่งแน่นอนว่ารวมถึงระบบคลาวด์ด้วย การเพิ่มขึ้นของมัลแวร์ที่อันตราย และการโจมตีในรูปแบบอื่น ๆ เช่นภัยคุกคามที่เลือกโจมตีไปที่เป้าหมายเฉพาะ (Advanced Persistent Threats: APTs) ที่ได้รับการออกแบบมาเพื่อให้สามารถหลบหลีกระบบป้องกันเครือข่ายได้ โดยกำหนดและมุ่งเป้าไปที่ช่องโหว่ต่าง ๆ ในคอมพิวติ้งสแต็ค การรั่วไหลของข้อมูลอาจเป็นสาเหตุให้ข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาตและเกิดการปลอมแปลงข้อมูล ซึ่งไม่มีโซลูชั่นใดที่จัดการกับภัยคุกคามเหล่านี้ได้อย่างชัดเจนนอกเสียจากว่าคุณจะต้องรับผิดชอบควบคุมระบบความปลอดภัยบนคลาวด์ให้ได้ด้วยวิธีการที่มีการพัฒนาให้ทันกับภัยคุกคามต่าง ๆ อยู่ตลอดเวลา

การรักษาความปลอดภัยในระบบคลาวด์เป็นความรับผิดชอบร่วมกัน

ไม่ว่าคุณจะใช้ระบบคลาวด์แบบใด คุณต้องรับผิดชอบต่อการรักษาความปลอดภัยในส่วนที่คุณใช้งานภายในระบบคลาวด์นั้น การใช้ระบบคลาวด์ที่ดูแลโดยบุคคลอื่นไม่ได้หมายความว่าคุณสามารถนิ่งนอนใจได้ การตรวจสอบที่ไม่มีประสิทธิภาพเพียงพอ จะเป็นสาเหตุสำคัญของความล้มเหลวในการรักษาความปลอดภัย การรักษาความปลอดภัยในระบบคลาวด์เป็นความรับผิดชอบของทุก ๆ คน ดังนี้

• ใช้ซอฟต์แวร์ที่เชื่อถือได้เท่านั้น
ซอฟต์แวร์ที่ใช้อยู่บนระบบคลาวด์ของคุณมีความสำคัญยิ่งเพราะเมื่อคุณดาวน์โหลดโค้ดใด ๆ จากแหล่งภายนอก คุณจะต้องทราบว่าโค้ดนั้นมีที่มาจากไหน ใครเป็นผู้สร้าง และมีโค้ดอันตรายอยู่ภายในหรือไม่ หากต้องการซอฟต์แวร์จะต้องจัดหาจากแหล่งที่รู้จัก เชื่อถือได้ และต้องให้มั่นใจว่ามีวิธีรักษาความปลอดภัยและติดตั้งการอัปเดตโปรแกรมในเวลาที่เหมาะสม

• เข้าใจเรื่องกฎระเบียบ
ข้อมูลส่วนบุคคล ข้อมูลการเงิน และข้อมูลที่ละเอียดอ่อนอื่น ๆ อาจจะอยู่ภายใต้กฎระเบียบที่เข้มงวด ซึ่งการบังคับใช้กฎหมายใด ๆ นั้นขึ้นอยู่กับว่าคุณทำธุรกิจที่ไหนกับใคร เช่น เมื่อคุณเห็นกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล (General Data Protection Regulation – GDPR) คุณจะต้องตรวจสอบการปฏิบัติตามกฎระเบียบก่อนที่จะเลือกใช้ระบบคลาวด์ใด ๆ เป็นต้น

• การบริหารจัดการไลฟ์ไซเคิล
สภาพแวดล้อมแบบคลาวด์เนทีฟทำให้การขึ้นตัวอย่างงานใหม่ ๆ เป็นไปได้อย่างง่ายดาย และในขณะเดียวกันตัวอย่างงานเก่า ๆ ก็จะถูกลืมไปได้ง่ายเช่นกัน ซึ่งงานหรือบริการที่ไม่ได้รับความสนใจสามารถกลายเป็นเหมือนซอมบี้บนคลาวด์แต่ปราศจากการตรวจสอบใด ๆ และอาจทำให้ล้าสมัยอย่างรวดเร็ว ซึ่งหมายความว่าไม่มีแพชรักษาความปลอดภัยใหม่ ๆ อัปเดตอีกต่อไป ซึ่งนโยบายการจัดการและการกำกับดูแลไลฟ์ไซเคิลสามารถช่วยในเรื่องนี้ได้

• พิจารณาความสามารถในการเคลื่อนย้าย
คุณสามารถย้ายเวิร์คโหลดไปยังระบบคลาวด์อื่นได้อย่างง่ายดายหรือไม่ ข้อตกลงระดับการให้บริการ (Service Level Agreement – SLA) ควรกำหนดไว้อย่างชัดเจนว่าผู้ให้บริการระบบคลาวด์จะคืนข้อมูลหรือแอปพลิเคชั่นของลูกค้าเมื่อใดและด้วยวิธีใด ถึงแม้ว่าคุณไม่ได้คิดจะย้ายข้อมูลหรือแอปพลิเคชั่นของคุณเร็ว ๆ นี้ก็ตาม แต่เพื่อป้องกันปัญหาการล็อคอินที่อาจเกิดขึ้นในวันข้างหน้า คุณจำเป็นจะต้องพิจารณาเรื่องการเคลื่อนย้ายข้อมูลในตอนนี้ด้วยเช่นกัน

• การตรวจสอบอย่างต่อเนื่อง
การตรวจสอบสิ่งที่เกิดขึ้นในเวิร์คสเปซของคุณจะช่วยให้คุณสามารถหลีกเลี่ยง หรืออย่างน้อยที่สุด ยับยั้งผลกระทบที่จะเกิดจากการละเมิดการรักษาความปลอดภัยได้ การจัดการแพลตฟอร์มคลาวด์แบบครบวงจร จะช่วยให้คุณสามารถตรวจสอบทรัพยากรทุกอย่างที่มีในทุกสภาพแวดล้อม

• เลือกผู้ให้บริการที่เหมาะสม
พิจารณาจัดจ้างและเป็นพาร์ทเนอร์กับผู้ให้บริการระบบคลาวด์ที่มีคุณสมบัติและไว้วางใจได้ และเข้าใจความซับซ้อนเรื่องการรักษาความปลอดภัยบนระบบคลาวด์ บางครั้งโครงสร้างพื้นฐานพับลิคคลาวด์อาจมีความปลอดภัยมากกว่าระบบไพรเวทคลาวด์ เนื่องจากผู้ให้บริการพับลิคคลาวด์มีทีมรักษาความปลอดภัยที่มีความพร้อมทั้งด้านข้อมูลและเครื่องมือดีกว่า

พับลิคคลาวด์ปลอดภัยหรือไม่

แม้จะบอกได้ถึงความแตกต่างด้านการรักษาความปลอดภัยที่ใช้ในระบบคลาวด์ทั้ง 3 แบบ ทั้งพับลิค ไพรเวท และไฮบริดคลาวด์ แต่สิ่งที่คนส่วนมากต้องการทราบก็คือ “พับลิคคลาวด์มีความปลอดภัยหรือไม่” ซึ่งคำตอบขึ้นอยู่กับปัจจัยหลายประการ

พับลิคคลาวด์มีการป้องกันที่เหมาะสมให้กับเวิร์กโหลดหลากหลายประเภท แต่ไม่ใช่กับทุกอย่าง ทั้งนี้เป็นเพราะส่วนใหญ่แล้วพวกเขาไม่ได้แยกจากไพรเวทคลาวด์ ระบบพับลิคคลาวด์รองรับการให้บริการผู้ใช้งานหลากหลายโดยไม่จำเป็นต้องอยู่องค์กรเดียวกันหรือใช้ซอฟต์แวร์เดียวกัน (Multitenancy) นั่นคือการที่คุณเช่าพื้นที่ในการเก็บข้อมูลจากผู้ให้บริการคลาวด์รายหนึ่งร่วมกับ “ผู้เช่า” รายอื่น ๆ ผู้เช่าแต่ละรายมีข้อตกลง SLA กับผู้ให้บริการคลาวด์ซึ่งระบุว่าใครรับผิดชอบอะไร ซึ่งก็เหมือนการเช่าห้องพักห้องหนึ่งจากเจ้าของบ้านเดียวกัน โดยเจ้าของบ้าน (ผู้ให้บริการคลาวด์) สัญญาว่าจะบำรุงรักษาอาคาร (โครงสร้างพื้นฐานคลาวด์) เป็นผู้ถือกุญแจอาคาร (การเข้าถึงข้อมูล) และโดยทั่วไปจะไม่มายุ่งกับผู้เช่า (ความเป็นส่วนตัว) และในอีกด้านหนึ่ง ผู้เช่าสัญญาว่าจะไม่ทำสิ่งใด (เช่น การใช้แอปพลิเคชั่นที่ไม่ปลอดภัย) ซึ่งอาจจะก่อให้เกิดความเสียหายแก่ตัวอาคาร หรือรบกวนผู้เช่ารายอื่น แต่คุณก็ไม่สามารถเลือกเพื่อนบ้านได้ และมีความเป็นไปได้อย่างยิ่งที่การเช่าพื้นที่นี้จะจบลงด้วยการที่เพื่อนบ้านคนใดคนหนึ่งนำสิ่งที่เป็นอันตรายเข้ามาสู่อาคาร แม้ว่าทีมรักษาความปลอดภัยด้านโครงสร้างพื้นฐานของผู้ให้บริการระบบคลา

วด์กำลังเฝ้าดูเหตุการณ์ที่ไม่ปกติอยู่ แต่ภัยคุกคามที่ซ่อนอยู่หรือมีความรุนแรง เช่น การโจมตีโดยปฏิเสธการให้บริการ (DDoS) ก็เกิดขึ้นได้ ซึ่งเป็นอันตรายต่อผู้เช่ารายอื่นเช่นกัน

อย่างไรก็ตาม นับเป็นเรื่องดีที่ยังมีมาตรฐานความปลอดภัย กฎระเบียบ และกรอบการควบคุมต่าง ๆ ซึ่งเป็นที่ยอมรับในอุตสาหกรรม เช่น Cloud Control Matrix จากองค์กร Cloud Security Alliance เป็นต้น คุณสามารถกันตัวเองออกจากสภาพแวดล้อมที่มีผู้เช่าหลายคนได้ ด้วยการเพิ่มมาตรการรักษาความปลอดภัย (เช่น การเข้ารหัส และเทคนิคการลดความเสี่ยงให้กับ DDoS) ซึ่งช่วยป้องกันเวิร์กโหลดจากโครงสร้างพื้นฐานที่ถูกบุกรุกได้ แต่หากมาตรการเหล่านี้ยังไม่เพียงพอ คุณสามารถใช้ระบบเชื่อมต่อระหว่างองค์กรไปยังระบบคลาวด์ (Cloud Access Security Brokers: CASB) เพื่อมอนิเตอร์กิจกรรมที่เกิดขึ้นและบังคับใช้นโยบายด้านความปลอดภัยต่าง ๆ เพื่อให้ฟังก์ชั่นการทำงานขององค์กรมีความเสี่ยงต่ำ อย่างไรก็ตามมาตรการที่กล่าวมาทั้งหมดนี้อาจจะไม่เพียงพอสำหรับองค์กรในอุตสาหกรรมที่ดำเนินงานภายใต้ข้อบังคับด้านความเป็นส่วนตัว การรักษาความปลอดภัย และการปฏิบัติตามกฎระเบียบที่เข้มงวด

ไฮบริดคลาวด์ช่วยลดความเสี่ยง

การตัดสินใจเรื่องการรักษาความปลอดภัยนั้น เกี่ยวข้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ และการวิเคราะห์ต้นทุน-กำไร ความเสี่ยงและผลประโยชน์ที่อาจเกิดขึ้นส่งผลต่อสถานภาพโดยรวมขององค์กรคุณอย่างไร อะไรคือสิ่งที่สำคัญที่สุด เวิร์กโหลดบางอย่างไม่ต้องการการเข้ารหัสและการรักษาความปลอดภัยระดับสูงสุด ซึ่งเปรียบได้กับการล็อคตัวบ้านของคุณจะทำให้สมบัติของคุณปลอดภัย แต่คุณอาจจะเลือกเก็บเฉพาะของมีค่ามากไว้ในตู้เซฟก็ได้ ซึ่งมันเป็นการดีที่มีทางเลือกให้ตัดสินใจ

ด้วยเหตุผลที่กล่าวมาข้างต้นทำให้องค์กรหันมาใช้ไฮบริดคลาวด์มากขึ้น ไฮบริดคลาวด์นำเอาคุณสมบัติที่ดีที่สุดของคลาวด์ทุกระบบมารวมไว้ให้คุณ ไฮบริดคลาวด์เป็นการรวมกันของสภาพแวดล้อมคลาวด์ที่เชื่อมต่อกันตั้งแต่ 2 ระบบขึ้นไป – คือพับลิคคลาวด์ หรือไพรเวทคลาวด์

ไฮบริดคลาวด์ช่วยให้คุณเลือกที่ที่คุณจะเก็บเวิร์กโหลดและข้อมูล เพื่อให้เป็นไปตามกฎระเบียบ การตรวจสอบนโยบาย หรือการรักษาความปลอดภัย คุณสามารถเลือกใช้งานเวิร์กโหลดที่มีความสำคัญเป็นพิเศษบนไพรเวทคลาวด์ โดยมีการใช้งานเวิร์กโหลดที่สำคัญน้อยกว่าในพับลิคคลาวด์แทน สำหรับระบบไฮบริดคลาวด์บางประเภทที่ไม่เหมือนใคร มีความท้าทายด้านการรักษาความปลอดภัยหลายอย่าง (เช่น การเคลื่อนย้ายข้อมูล ความซับซ้อนที่เพิ่มขึ้นและมีช่องทางที่จะถูกโจมตีมาก แต่การมีสภาพแวดล้อมที่หลากหลายก็สามารถนำมาใช้เป็นหนึ่งในการป้องกันความเสี่ยงด้านการรักษาความปลอดภัยที่แข็งแกร่งที่สุดได้