**รายงานสรุปผลการปฏิบัติงาน  
 ศูนย์เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศ**

**(Security Operation Center)**

**ประจำเดือน มีนาคม 2565**

**สภากาชาดไทย**

**ประวัติการแก้ไขเอกสาร**

| **เวอร์ชัน** | **รายละเอียด** | **ผู้จัดทำ** | **วันที่อนุมัติ** |
| --- | --- | --- | --- |
| 1.0 | จัดทำร่างเอกสาร | ศูนย์ SOC | 1 กันยายน 2562 |
| 1.1 | จัดทำภาคผนวก | ศูนย์ SOC | 10 พฤศจิกายน 2563 |

**สารบัญ**

**หัวข้อ หน้า**

[หลักการและเหตุผล 4](#_Toc97279328)

[วัตถุประสงค์ 4](#_Toc97279329)

[บทสรุปสำหรับผู้บริหาร 5](#_Toc97279330)

[ภาพรวมของการเฝ้าระวังเหตุการณ์ด้านความปลอดภัย (Security Incident) 5](#_Toc97279331)

[สรุปจำนวนอุปกรณ์ที่ส่ง Log 9](#_Toc97279332)

[สรุปค่าเฉลี่ยจำนวน Log 9](#_Toc97279333)

[ภาคผนวก 10](#_Toc97279334)

**รายงานสรุปผลการดำเนินงานของศูนย์เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศ**

**ประจำเดือน มีนาคม 2565**

**เสนอ**

**สภากาชาดไทย**

**จัดทำโดย บริษัท ไอเน็ต แมเนจด์ เซอร์วิสเซส จำกัด**

## หลักการและเหตุผล

ในปัจจุบันหน่วยงาน หรือ องค์กรต่าง ๆ มีการนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ร่วมกับระบบงานต่าง ๆ อย่างแพร่หลาย เพื่อลดระยะเวลา เพิ่มประสิทธิภาพในการปฏิบัติงาน หรือแม้แต่การเสริมสร้างภาพลักษณ์ขององค์กร แก่ผู้ใช้บริการ เช่น การจัดทำเว็บไซต์ของหน่วยงาน เป็นต้น เครื่องให้บริการ (Server) อุปกรณ์ระบบเครือข่าย (Network) และระบบปฏิบัติการ (Operating System) เป็นองค์ประกอบที่สำคัญที่จะทำให้ระบบสารสนเทศสามารถให้บริการแก่ผู้ใช้บริการ อย่างไรก็ตาม เพื่อให้ระบบสารสนเทศสามารถให้บริการได้อย่างมีประสิทธิภาพ สิ่งที่สำคัญที่องค์กรจะขาดไม่ได้ คือ เจ้าหน้าที่ดูแลระบบสารสนเทศที่มีความเชี่ยวชาญในระบบสารสนเทศ มีความรู้ ความเข้าใจทั้งในเรื่องความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และ การแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในสถานการณ์เฉพาะหน้าในระบบงาน ที่ให้บริการแก่สาธารณะ หรือบุคลากรขององค์กร ในการให้บริการของระบบงานนั้น อาจมีกลุ่มคน ผู้ไม่ประสงค์ดีปะปน เข้ามาใช้บริการกับผู้ใช้งานทั่วไป เป็นเหตุให้ระบบเกิดความล่าช้า หรือไม่สามารถให้บริการแก่ผู้ใช้บริการได้อย่างมีประสิทธิภาพ ไปจนถึงการจารกรรมข้อมูล ซึ่งอาจจะก่อให้เกิดความเสียหายที่อาจจะประเมินมูลค่าไม่ได้

โดยการป้องกันเหตุการณ์เหล่านี้ จำเป็นจะต้องได้รับความร่วมมือหลาย ๆ ส่วน ไม่ว่าจะเป็นเจ้าของระบบงานนั้น ๆ ไปจนถึงผู้ให้บริการ ในการให้ความร่วมมือเพื่อป้องกันเหตุการณ์ที่อาจจะเกิดขึ้นและตรวจสอบเมื่อมีเหตุการณ์เกิดขึ้นแล้ว พร้อมด้วยความที่บุคลากรทางด้านเทคโนโลยีสารสนเทศของหน่วยงานนั้น อาจจะมีความตระหนักรู้ทางด้านความมั่นคงปลอดภัยสารสนเทศไม่เพียงพอ จึงมีความจำเป็นที่จะต้องมีหน่วยงานที่จะสามารถประสานงาน ให้ความรู้ และช่วยเสริมสร้างให้ระบบงาน บุคลากร ไปจนถึงภาพรวมของหน่วยงาน มีความมั่นคงปลอดภัยสารสนเทศ ที่เพิ่มมากขึ้น โดยอ้างอิงมาตรฐานสากลเพื่อให้มีความน่าเชื่อถือ และสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงานให้ยั่งยืนต่อไป

## วัตถุประสงค์

1. เพื่อให้มั่นใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น จะได้รับการเฝ้าระวัง และแจ้งเตือนได้อย่างมีประสิทธิภาพ ตรงตามขอบเขตการดำเนินงานที่บริษัทฯ ได้รับมอบหมายภายในสัญญาภายใต้โครงการฯ
2. เพื่อปฏิบัติ และดำเนินงานได้อย่างถูกต้องครบถ้วนตามขอบเขตของข้อกำหนดในโครงการฯ

## บทสรุปสำหรับผู้บริหาร

บริษัทฯ ได้สรุปเหตุการณ์การด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศที่เกิดขึ้นในเดือน มีนาคม 2565 โดยมีรายละเอียดดังนี้

### ภาพรวมของการเฝ้าระวังเหตุการณ์ด้านความปลอดภัย (Security Incident)

จากผลการเฝ้าระวังประจำเดือนมีนาคม 2565 ตรวจพบเหตุการณ์ที่สำคัญ ดังรายละเอียด ต่อไปนี้

| **ลำดับ** | **ชื่อหน่วยงาน** | **จำนวนเหตุการณ์** | **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | สภากาชาดไทย | 14 | 2 | 2 | 10 | - |

มีเหตุการณ์ที่น่าสนใจดังนี้

1. ตรวจพบเหตุการณ์ Outbound Communication With Blacklist IP Address คือเหตุการณ์ที่อุปกรณ์ภายในองค์กรทำการเชื่อมต่อไปยังเครื่องปลายทางที่เป็น IP อันตราย ( Blacklist IP )

| **Source IP** | **Destination IP** | **Destination Geolocation** | **Destination Port** | **Event Subtype** | **Time** |
| --- | --- | --- | --- | --- | --- |
| 10.189.191.66 | 74.82.46.26 | Singapore | 3545 | Pass | 2022/03/01 09:38:24 น. |
| 10.188.1.86 | 14.1.112.177 | Singapore | 38376 | Pass | 2022/03/21 07:02:49 น. |

**คำแนะนำ**

* ดำเนินการตรวจสอบเครื่องต้นทางที่มีการเชื่อมต่อกับอุปกรณ์ปลายทางที่เป็นอันตรายซึ่งอยู่ใน Blacklist IP หรือ เครื่องเป้าหมายอาจติด Malware ทำให้มีการเชื่อมต่อไปกับ IP อันตราย ( Blacklist IP )
* ทำการ Full Scan เพื่อตรวจสอบว่าเครื่องเป้าหมายถูกติดตั้ง Malware ไว้หรือไม่ และทำ Policy Firewall ไม่ให้มีการติดต่อกันของ IP ต้นทางและ IP ปลายทางที่เป็นอันตราย

1. พบเหตุการณ์ SSH Access from Suspicious IP คือเหตุการณ์ที่ตรวจพบ Traffic จากอุปกรณ์ภายนอกที่เป็น IP อันตราย ( Blacklist IP ) เชื่อมต่อมายังเครื่องปลายทางที่เป็นเครื่องภายในองค์การด้วย Port SSH ( 22 )

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source IP** | **Source Geolocation** | **Destination IP** | **Event**  **Subtype** | **Time** |
| 64.62.197.122 | United States | 10.188.1.46 | Pass | 2022/03/08 20:15:59 **น.** |
| **159.65.140.76** | Singapore | 10.188.1.82 | pass | **2022/03/31 06:35:11 น.** |

คำแนะนำ

* ตรวจสอบเครื่องปลายทางว่ามีการเปิดให้บริการหมายเลข Port : SSH ( 22 ) หรือไม่
* ทำการเปิดเฉพาะหมายเลข Port ที่ให้บริการหรือที่จำเป็นเท่านั้น
* ให้ทำการ Block Traffic หมายเลข IP ของผู้บุกรุกบน firewall
* หากมีการเปิดให้บริการและมีความจำเป็นต้องให้บริการโดยส่วนตัว ให้พิจารณาเปิดการเข้าถึงเฉพาะหมายเลข IP ที่ได้รับอนุญาตหรือทำการต่อ VPN ก่อนเข้าถึงบริการส่วนตัว
* ควรมีการพิจารณา Update Patch/Hotfix ของ Software ที่เปิดให้บริการอยู่เสมอ เพื่อลดความเสี่ยงของการโจมตีจากช่องโหว่ต่าง ๆ

1. ตรวจพบเหตุการณ์ Inbound Communication With Blacklist IP Address  เป็นเหตุการณ์ที่อุปกรณ์ภายนอกองค์กรและเป็น IP อันตราย ( Blacklist IP ) ทำการเชื่อมต่อเข้ามายังอุปกรณ์ภายในองค์กร

| **Source IP** | **Source Geolocation** | **Destination IP** | **Destination Port** | **Event Subtype** | **Time** |
| --- | --- | --- | --- | --- | --- |
| 124.133.28.21 | China | 10.188.128.62 | 3306 | pass | 2022/03/04 17:17:40 น. |
| 71.6.135.131 | United States | 10.188.1.81 | 443 | pass | 2022/03/08 22:49:17 น. |
| 167.248.133.60 | United States | 10.188.128.246 | 8081 | pass | 2022/03/10 12:47:19 น. |
| 222.186.46.200 | China | 10.188.128.246 | 8888 | pass | 2022/03/10 23:09:42 น. |
| 167.248.133.117 | United States | 172.16.33.22 | 81 | pass | 2022/03/12 09:17:20 น. |
| 167.248.133.46 | United States | 172.19.1.109 | 2000 | pass | 2022/03/18 21:02:36 น. |
| 134.122.134.161 | Japan | 10.188.1.19 | 10000 | pass | 2022/03/25 06:13:22 น. |
| 94.102.49.193 | Netherlands | 10.188.128.162 | 443 | pass | 2022/03/26 16:00:35 น. |
| 23.224.186.179 | United States | 10.188.128.62 | 8083 | pass | 2022/03/28 00:17:40 น. |
| 182.176.91.80 | Pakistan | 10.188.128.90 | 1433 | pass | 2022/03/28 13:00:47 น. |

**คำแนะนำ**

* ดำเนินการตรวจสอบเครื่องเป้าหมายที่มีการโจมตีเข้ามาว่ามีการเปิดใช้งาน Service ที่สามารถเข้าถึงได้จากภายนอกหรือไม่
* ทำการตรวจสอบเครื่องเป้าหมายว่ามีความจำเป็นที่จะต้องใช้งาน Port ดังกล่าวหรือไม่ หากไม่มีความจำเป็นให้ดำเนินการปิดการใช้งาน
* หากมีความจำเป็นต้องใช้งาน Port ให้พิจารณาทำการอนุญาตให้เฉพาะหมายเลข IP ที่ไว้ใจสามารถเข้าถึงหมายเลข Port และ Service นั้นได้
* ทำ Policy Firewall ให้อนุญาตเข้าถึงเฉพาะหมายเลข Port ที่เครื่องภายในองค์กรเปิดให้บริการ

สรุปเหตุการณ์ด้านความปลอดภัย โดยแสดงสถานะ ระดับความรุนแรง ผลกระทบ และ Top 10 Incidents

|  |  |  |
| --- | --- | --- |
| **ประเภทของภัยคุกคาม** | **ระดับความรุนแรง** | **จำนวนเหตุการณ์** |
|  |
| **Suspicious Activity** | | **12** |  |
| Outbound Communication with Blacklist IP Address - Pass | CRITICAL | 2 |  |
| SSH Access from Suspicious IP | HIGH | 2 |  |
| Inbound Communication with Blacklist IP Address | MEDIUM | 10 |  |
| **รวม** | | **14** |  |

สรุปแนวโน้มการโจมตี

Chart

Description automatically generated

แสดงสถิติเหตุการณ์การโจมตีในแต่ละเดือน

**สรุปจำนวนอุปกรณ์ที่ส่ง Log**

| **No.** | **Device Name** | **Device Type** | **IP Address** | **Remark** |
| --- | --- | --- | --- | --- |
| 1. | Firewall-A | Firewall | 192.168.9.109 |  |
| 2. | Firewall-A | Firewall | 192.168.9.107 |  |
| 3. | TRCSHOSTING02 | Server | 10.188.1.86 |  |
| 4. | TRCSHOSTING03 | Server | 10.188.1.89 |  |
| 5. | SOOKJAI | Server | 10.188.1.81 |  |
| 6. | mecfolio | Server | 10.188.1.71 |  |
| 7. | Museum | Server | 10.188.1.51 |  |
| 8. | First Aid Training | Server | 10.188.1.123 |  |
| 9. | MSSQL2017 | Server | 10.188.129.50 |  |
| 10. | MSSQL2019 | Server | 10.188.129.45 |  |
| 11. | VTRIS | Server | 10.188.128.83 |  |
| 12. | ORGAN-2017 | Server | 10.188.128.75 |  |
| 13. | e-service | Server | 10.188.128.52 |  |

### สรุปค่าเฉลี่ยจำนวน Log

|  |  |
| --- | --- |
| **ชื่อหน่วยงาน** | **หน่วย GB/Day** |
| สภากาชาดไทย | 20.07019 |

**ภาคผนวก**

| **No.** | **Category** | **Name** | **Description** | **Priority** |
| --- | --- | --- | --- | --- |
| 1 | Suspicious Activity | DDoS Outbound Flood Traffic | เกิดเหตุการณ์มีการเชื่อมต่อจากภายในหน่วยงานหลายเครื่องออกไปสู่ภายนอก เกิดจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 2 | Suspicious Activity | Denial of Service Attack - External | เกิดเหตุการณ์การแจ้งเตือนเมื่อพบการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้ โดยมี Traffic เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 3 | Suspicious Activity | Denial of Service Attack - Internal | เกิดเหตุการณ์การแจ้งเตือนเมื่อพบการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้ โดยมี Traffic เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 4 | Suspicious Activity | Distributed Denial of Service Attack | เกิดเหตุการณ์การแจ้งเตือนเมื่อพบการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้ โดยมี Traffic เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 5 | Suspicious Activity | DoS Outbound Flood Traffic | เกิดเหตุการณ์มีการเชื่อมต่อจากภายในหน่วยงานออกไปสู่ภายนอกจำนวนหลายเครื่อง เกิดจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 6 | Suspicious Activity | Outbound Communication with Blacklist IP Address - Pass | เกิดเหตุการณ์การเชื่อมต่อจากอุปกรณ์ภายในออกไปยังจากอุปกรณ์ภายนอกที่มี IP Blacklist โดย Firewall ทำการปล่อยผ่าน Traffic | Critical (P1) |
| 7 | Malware | Mimikatz Detect | ตรวจพบโปรแกรมที่เป็นอันตรายชื่อ Mimikatz จาก Log อุปกรณ์ | High (P2) |
| 8 | Malware | Virus or Spyware Detected but Failed to Clean | เกิดเหตุการณ์แจ้งเตือน เมื่อตรวจพบ Log จาก Anti-Virus หรือ Anti-Spyware ว่ามีการแพร่กระจาย Malware ชนิดเดียวกัน จาก file เดียวกัน ภายในเครื่องเดียวกัน เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | High (P2) |
| 9 | Server Compromise | Brute force Login Attack (Success) | เกิดเหตุการณ์ที่กรอกรหัสผ่านสำเร็จ ภายในจำนวนครั้งที่กำหนด | High (P2) |
| 10 | Suspicious Activity | Outbound Communication with Blacklist IP Address - Block | เกิดเหตุการณ์การเชื่อมต่อจากอุปกรณ์ภายในออกไปยังจากอุปกรณ์ภายนอกที่มี IP Blacklist โดย Firewall ทำการ BlockTraffic | High (P2) |
| 11 | Suspicious Activity | Outbound Communication with Suspicious URL | ตรวจพบเหตุการณ์การเชื่อมต่อของอุปกรณ์กับ URL ที่เป็นอันตราย | High (P2) |
| 12 | Suspicious Activity | Outbound Flood Traffic | เกิดเหตุการณ์มีการเชื่อมต่อจากภายในหน่วยงานออกไปสู่ภายนอกเกิดจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | High (P2) |
| 13 | Suspicious Activity | RDP Traffic Access from Suspicious IP | ตรวจสอบพบเหตุการณ์ มีการเชื่อมต่อจากภายนอก Blacklist IP เข้ามาที่เครื่องภายในองค์กรด้วย Port RDP 3389 | High (P2) |
| 14 | Suspicious Activity | SSH Traffic Access from Suspicious IP | ตรวจสอบพบเหตุการณ์ มีการเชื่อมต่อจากภายนอก Blacklist IP เข้ามาที่เครื่องภายในองค์กรด้วย Port SSH 22 | High (P2) |
| 15 | System Error | Monitored Log Source Stopped Sending Events | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบว่าอุปกรณ์หยุดการส่ง Log มายังระบบเกินกว่า ระยะเวลาที่กำหนด | High (P2) |
| 16 | Web Compromise | Cross site script (Custom) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Cross site script โดยตรวจจับผ่าน Log web access | High (P2) |
| 17 | Web Compromise | Cross site script (System Detected) Pass | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Cross site script โดยตรวจจับผ่าน WAF | High (P2) |
| 18 | Web Compromise | Directory Traversal (Custom) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Directory Traversal โดยตรวจจับผ่าน Log web access | High (P2) |
| 19 | Web Compromise | Directory Traversal (System Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Directory Traversal โดยตรวจจับผ่าน WAF | High (P2) |
| 20 | Web Compromise | SQL Injection (Custom Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการSQL Injection ตรวจจับผ่าน Log web access | High (P2) |
| 21 | Web Compromise | SQL Injection (System Detect) Pass | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ SQL Injection โดยตรวจจับผ่าน WAF | High (P2) |
| 22 | Malware | Virus or Spyware Detected | เกิดเหตุการณ์การแจ้งเตือนจากโปรแกรม Anti-Virus หรือ Anti-Spyware ว่ามีการแพร่กระจาย Malware ภายในเครือข่าย | Medium (P3) |
| 23 | Server Compromise | Brute force Login Attack (Failed) | เกิดเหตุการณ์ที่กรอกรหัสผ่านไม่สำเร็จเกินจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | Medium (P3) |
| 24 | Suspicious Activity | Host Sending Excessive Email | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบ Host ที่ไม่ได้กำหนดให้เป็น Mail Server พยายามส่ง E-mail ไปยัง Host เดียว หรือ หลาย Host มากผิดปกติ | Medium (P3) |
| 25 | Suspicious Activity | Inbound Communication with Blacklist IP Address | เกิดเหตุการณ์การเชื่อมต่อมาจากอุปกรณ์ที่มี IP Blacklist ภายนอกองค์กรมายังอุปกรณ์ภายในองค์กร | Medium (P3) |
| 26 | Web Compromise | Cross site script (System Detected) Block | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Cross site script โดยตรวจจับผ่าน WAF | Medium (P3) |
| 27 | Web Compromise | Directory Traversal (System Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Directory Traversal โดยตรวจจับผ่าน WAF | Medium (P3) |
| 28 | Web Compromise | SQL Injection (System Detect) Block | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ SQL Injection โดยตรวจจับผ่าน WAF | Medium (P3) |
| 29 | Web Compromise | Suspicious Post from Untrusted Source | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบการเข้าถึง URL ที่มีความผิดปกติ | Medium (P3) |
| 30 | Information Gathering | High Threat Targeting Vulnerable Asset | เกิดเหตุการณ์พยายามโจมตีเข้าสู่ระบบที่มีความเสี่ยงสูง หรือมีช่องโหว่อยู่ | Low (P4) |
| 31 | Information Gathering | Port Scan | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบการพยายาม Scan Port ต่าง ๆ หลาย Port ไปยังเครื่องเป้าหมายเครื่องเดียว เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Low (P4) |
| 32 | Information Gathering | Port Sweep | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบ การพยายาม Scan เครือข่าย โดยการเจาะจง Port ไปยังเครื่องต่าง ๆ เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Low (P4) |
| 33 | Information Gathering | Vulnerability Scanner Detected (by events) | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบการ Scan ค้นหาช่องโหว่ของระบบ | Low (P4) |