# พรบ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

# และ

# การ Implement Cyber Security for University

---

วันที่ 24 พฤษภาคม 2566 เวลา 9.00 – 12.00 น.
มหาวิทยาลัยเชียงใหม่


โดย
**นายภาณุพงษ์ ธนูทอง**
ผู้อำนวยการฝ่ายบริหารความมั่นคงปลอดภัย
รักษาการผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)


ข้อมูลวันที่ 24 พฤษภาคม 2566

## วิทยากร


### นายภาณุพงษ์ ธนูทอง

**ผู้อำนวยการฝ่ายบริหารความมั่นคงปลอดภัย**
**รักษาการผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ**
**สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)**
**โทร 02-502-7808 อีเมล panupong.t@ncsa.or.th**


## ประวัติการศึกษา

**วิศวกรรมศาสตร์บัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ ม.เทคโนโลยีพระจอมเกล้าธนบุรี**
**วิศวกรรมศาสตร์บัณฑิต สาขาวิศวกรรมโยธา ม.ศรีปทุม**
**Master of Engineering in Information and Communication Technology for Embedded Systems TAIST-Tokyo Tech**

## ประสบการณ์ด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

- **อดีตวิศวกร กองสารสนเทศภูมิศาสตร์, กองบริหารเครือข่ายสื่อสารและความมั่นคงสารสนเทศ การประปานครหลวง**
- **ช่วยราชการ ทีมงานจัดตั้ง สกมช. และ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ**
- **ร่วมจัดทำระบบเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของ สกมช.**
- **พนักงานเจ้าหน้าที่ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550**
- **พนักงานเจ้าหน้าที่ตาม พรบ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**
- **เจ้าหน้าที่จัดการแข่งขัน การแข่งขันทักษะทางไซเบอร์ Thailand Cyber Top Talent 2022**
- **เจ้าหน้าที่จัดการฝึก Thailand's National Cyber Exercise 2022**

# ประวัติความเป็นมา สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ


ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 ให้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐที่มีหน้าที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบและสร้างความเดือดร้อนต่อประชาชน ตลอดจนความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ

หน้าที่ของ สกมช. คือ รับผิดชอบงานตามพระราชบัญญัติ ประสานงานร่วมกันทั้งภาครัฐและเอกชน รวมถึงกำหนดนโยบาย ระเบียบ มาตรฐานขั้นต่ำแนวทางความปลอดภัยสำหรับหน่วยงานรัฐ ป้องกันรับมือภัยคุกคามไซเบอร์ ตลอดจนความมั่นคงของรัฐและความสงบเรียบร้อยของประเทศ ตั้งเป้าระยะสามปีคือการสร้างบุคลากรด้านไซเบอร์ซีเคียวริตี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีตัวย่อว่า สกมช. และมีชื่อภาษาอังกฤษ “The National Cyber Security Agency (NCSA)” เป็นหน่วยงานของรัฐในรูปแบบองค์การมหาชน ซึ่งมุ่งเน้นการบริหารและดำเนินงานอย่างมีประสิทธิภาพ เพื่อเป็นหน่วยงานกลาง สร้างกลไกขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือ สนับสนุน ให้ความรู้ ความเข้าใจ ให้หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และประชาชน เพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น

# เกี่ยวกับ สกมช.

## วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

## พันธกิจ MISSIONS

เสนอแนะนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดแนวทาง มาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

# บทบาทของ สกมช.

**ขับเคลื่อน**

การพัฒนาแผนการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

**บังคับใช้กฎหมาย**

การบังคับใช้ พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองภายใต้ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

**ส่งเสริมความร่วมมือ**

การส่งเสริมความร่วมมือระหว่างประเทศและหน่วยงานภายในประเทศ

**เฝ้าระวังตอบโต้**

การเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์

**พัฒนา**

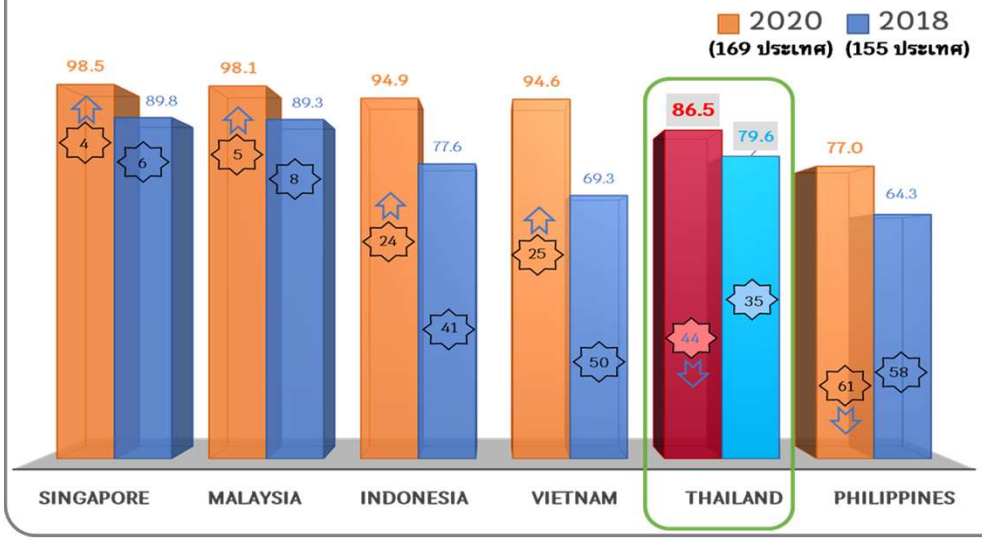
การพัฒนาหลักสูตรบุคลากรตลอดจนการสร้างการตระหนักรู้

**ยกระดับ**

การยกระดับขีดความสามารถของหน่วยงานภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

# ปัจจุบัน ประเทศไทย อยู่ตรงไหน?

ผลการจัดอันดับ Global Cybersecurity Index (GCI) 2020 หรือดัชนีความมั่นคงปลอดภัยไซเบอร์โลก โดย ITU




| Year 2020 | Singapore | Malaysia | Indonesia | Vietnam | Thailand | Philippines |
|---|---|---|---|---|---|---|
| Legal | 20.0 | 20.0 | 18.5 | 20.0 | **19.1** | 20.0 |
| Technical | 19.5 | 19.1 | **19.1** | **16.3** | **15.6** | 13.0 |
| Organizational | 19.0 | 19.0 | 17.8 | 19.0 | **17.6** | 11.9 |
| Capacity Development | 20.0 | 20.0 | **19.5** | **19.3** | **16.8** | 12.7 |
| Cooperative | 20.0 | 20.0 | 20.0 | 20.0 | 17.3 | 19.4 |
| | **98.5** | **98.1** | **94.9** | **94.6** | **86.5** | **77.0** |

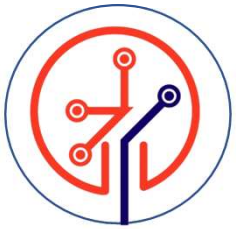
ปี 2018 ไทยอยู่ลำดับที่ 35 แต่ในปี 2020 อยู่ลำดับที่ 44 ของโลก แม้ในภาพรวมคะแนนจะสูงขึ้น แต่เนื่องจากประเทศอื่น ๆ ทำคะแนนได้สูงขึ้นมาก อย่างในภูมิภาคเอเชียตะวันออกเฉียงใต้ ทั้งอินโดนีเซียและเวียดนาม ทำให้ในปี 2020 ประเทศไทยตกไปอยู่ในลำดับที่ 5 ของภูมิภาค จากเดิมในปี 2018 ประเทศไทยอยู่ลำดับที่ 3 ของภูมิภาค

# วิสัยทัศน์

"เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุก

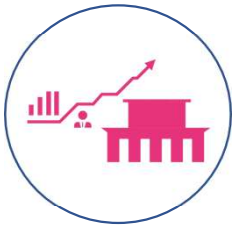
# พันธกิจ

เสนอแนะและขับเคลื่อนนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง ศึกษาวิจัย กำหนดแนวทาง มาตรฐาน มาตรการ ที่ เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต



กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้ง ส่งเสริม สนับสนุน และ ช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์



เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เสนอแนะและขับเคลื่อนนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง ศึกษาวิจัย กำหนดแนวทาง มาตรฐาน มาตรการ ที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

## ยุทธศาสตร์ที่ 1

สร้าง **Ecosystem** ที่เอื้อต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

### เป้าหมายยุทธศาสตร์

ประเทศไทยมี **Ecosystem** ที่เอื้อต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการพึ่งพาตนเองในอนาคตอย่างยั่งยืน

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

## ยุทธศาสตร์ที่ 2

ยกระดับ และเพิ่มขีดความสามารถในการประสานงานป้องกันและรับมือภัยคุกคามทางไซเบอร์ในทุกระดับและทุกกลุ่มเป้าหมาย

### เป้าหมายยุทธศาสตร์

ประเทศไทยมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานทุกภาคส่วนที่มีความพร้อมในการประสานงานป้องกัน และรับมือภัยคุกคามทางไซเบอร์ในทุกมิติ

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐ และเอกชน ทั้งในประเทศและต่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

## ยุทธศาสตร์ที่ 3

การสร้างความตระหนักรู้ให้กับประชาชน และ การสานพลังเครือข่ายความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

### เป้าหมายยุทธศาสตร์

ประชาชนทุกช่วงวัยมีความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์รวมทั้งมีการประสานงานเครือข่ายเพื่อบูรณาการให้บุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของทุกภาคส่วนมีขีดความสามารถในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

เผยแพร่ความรู้ ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

## ยุทธศาสตร์ที่ 4

พัฒนาสู่ องค์กรสมรรถนะสูง
(High-Performance Organization: HPO)

### เป้าหมายยุทธศาสตร์

สกมช. เป็นองค์กรชั้นนำมีบุคลากรที่มีสมรรถนะสูงและเป็นผู้นำในการปฏิบัติงานด้วยเทคโนโลยีและนวัตกรรมที่ทันสมัยเป็นที่ยอมรับในระดับสากล

### กลยุทธ์ที่ 1
**พัฒนา และขับเคลื่อน** นโยบาย แผนมาตรฐาน และแนวปฏิบัติ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

### กลยุทธ์ที่ 2
ส่งเสริม**การให้บริการ** และอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

### กลยุทธ์ที่ 3
ส่งเสริม**การวิจัย** เพื่อสร้างองค์ความรู้ และเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์

### กลยุทธ์ที่ 4
**ยกระดับ**ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการประสานงานป้องกัน และรับมือภัยคุกคามทางไซเบอร์

### กลยุทธ์ที่ 5
**ขีดความสามารถ** และ**สร้างแรงจูงใจ** ให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล(Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ(CII) และส่วนงาน (Sectoral CERT) ในการประสานงานป้องกัน และรับมือภัยคุกคามทางไซเบอร์

### กลยุทธ์ที่ 6
**ทบทวน พัฒนา ปรับปรุง** กฎหมายและมาตรการการบังคับใช้ เพื่อให้มีเครื่องมือและกลไกในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

### กลยุทธ์ที่ 7
เสริมสร้างความรู้ความเข้าใจและ**สร้างความตระหนักรู้แก่ประชาชน**

### กลยุทธ์ที่ 8
**ขยายเครือข่ายความร่วมมือ**หน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศ หรือนานาชาติ เพื่อสร้างความเข้มแข็งในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

### กลยุทธ์ที่ 9
**นำองค์กรด้วยเทคโนโลยี** และวัตกรรมที่ทันสมัย เพื่อการบริหารงานที่ยืดหยุ่นคล่องตัว และมีประสิทธิภาพ

### กลยุทธ์ที่ 10
พัฒนาระบบการจัดการทรัพยากรมนุษย์และ**เพิ่มขีดความสามารถบุคลากร**สู่ความเป็นผู้นำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

### กลยุทธ์ที่ 11
แสวงหารายได้จากแหล่งงบประมาณอื่น เพื่อ**การพัฒนาที่ยั่งยืน**

“ตอนนี้มีการตื่นตัวเรื่องภัยคุกคามทางโซเบอร์เยอะขึ้น ซึ่งประเด็นนี้ไม่ใช่แค่เรื่องเทคโนโลยีและอุปกรณ์ แต่ยังเป็นเรื่องกระบวนการบริหารจัดการที่ดี ทั้ง นโยบาย แผนการ และบุคลากร”

https://www.ncsa.or.th/article.html

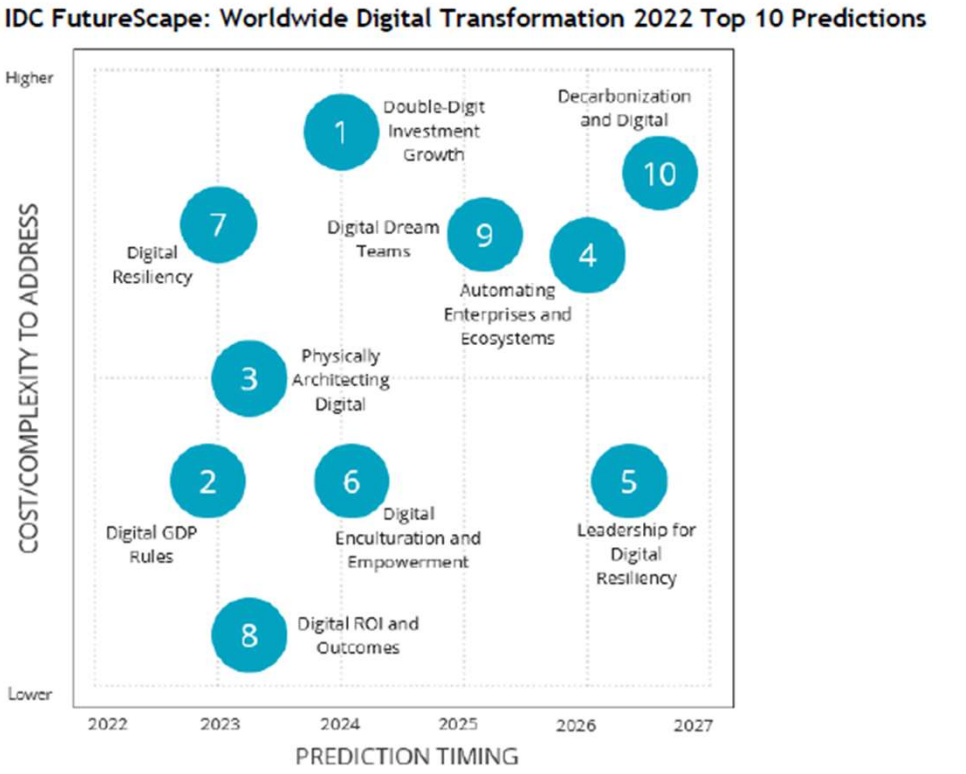
**พลอากาศตรีอมร ชมเชย**

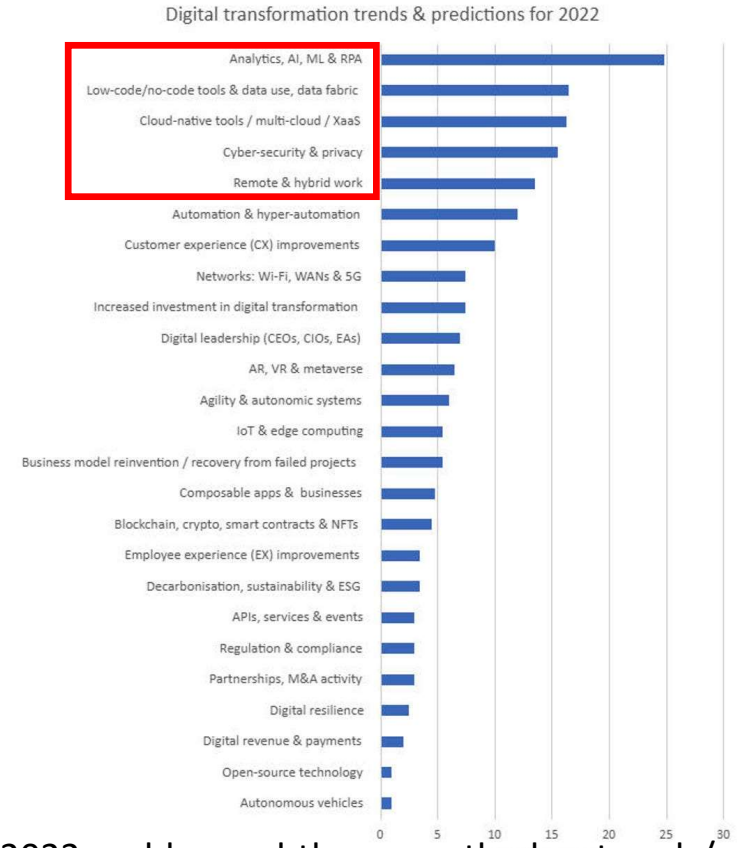
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กล่าวตอนหนึ่งในในงานสัมมนา “ ไทยกับความปลอดภัยไซเบอร์ 2022 “ เมื่อวันที่ 30 มีนาคม 2565

# สถานการณ์และแนวโน้มเกี่ยวกับ
# ภัยคุกคามทางไซเบอร์

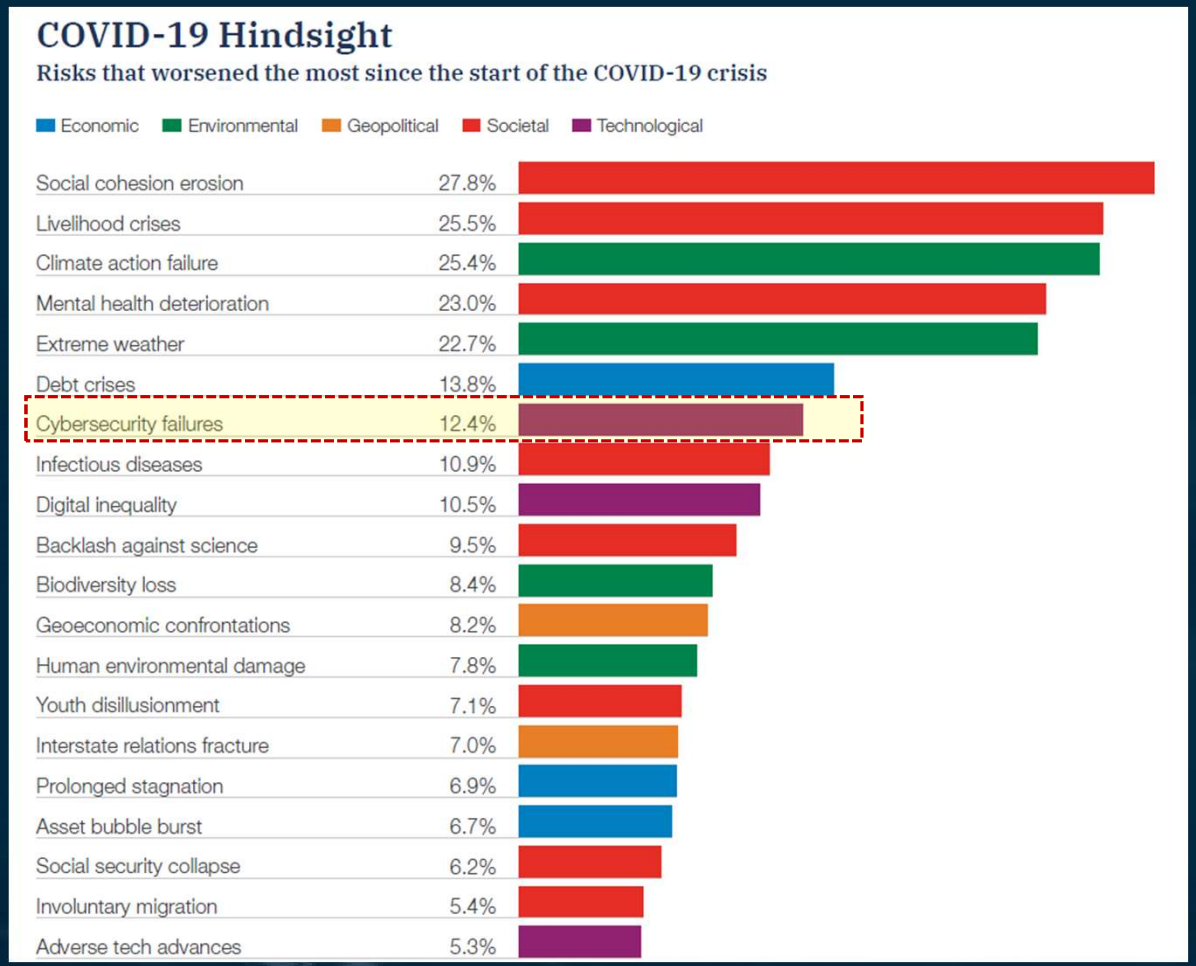
# Worldwide Digital Transformation




Source: https://www.zdnet.com/article/digital-transformation-in-2022-and-beyond-these-are-the-key-trends/
https://www.linkedin.com/pulse/worldwide-digital-transformation-predictions-2022-mehmet-mu%C5%9Ftal%C4%B1/

# แนวโน้มภัยคุกคามทางไซเบอร์

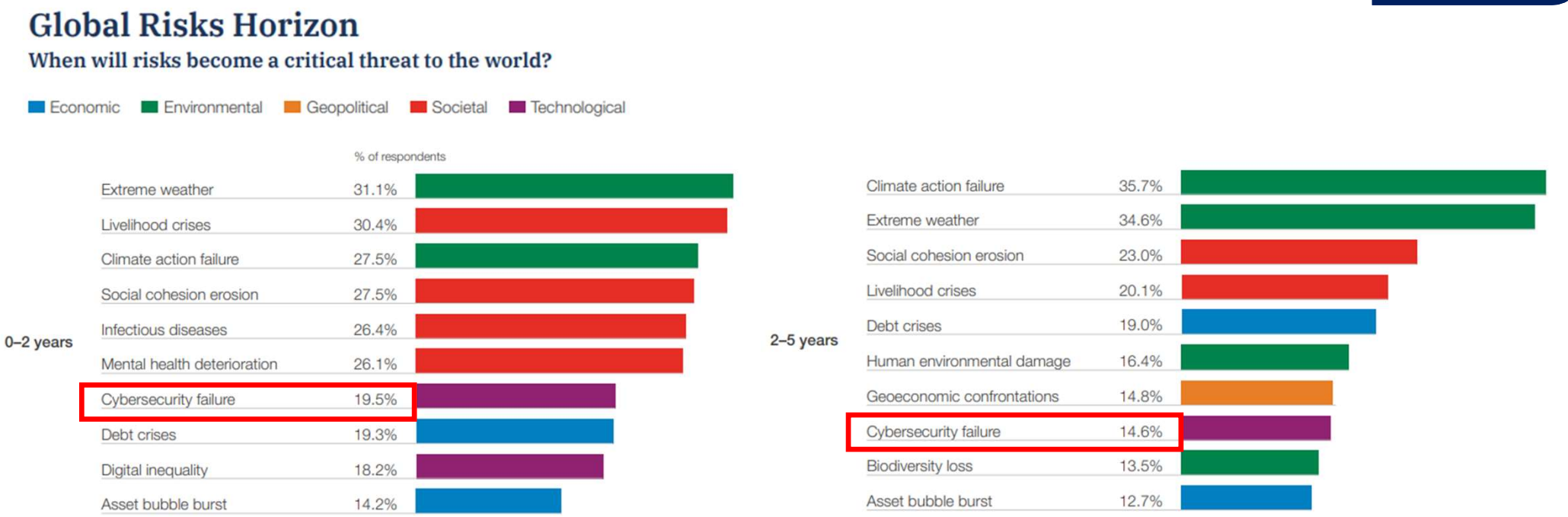



**"Cybersecurity failures"**

**ติดอันดับ 7** ของความเสี่ยงที่เลวร้ายที่สุดตั้งแต่เริ่มวิกฤต COVID-19 และเป็น **อันดับที่ 1** ของความเสี่ยงในหมวดเทคโนโลยี

Reference: World Economic Forum – The Global Risks Report 2022

# แนวโน้มภัยคุกคามทางไซเบอร์




Source: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

# สถิติการใช้งาน Internet ของประเทศไทย

## Top 10 กิจกรรมออนไลน์ยอดฮิตของคนไทย

มีการเติบโตจากปีที่ผ่านมาในทุกกิจกรรม

**Social Media ครองอันดับ 1**
กิจกรรมยอดฮิต **8 ปีซ้อน**

**เรียนออนไลน์ (e-Learning)**
**กลับมาติด Top 10 ในรอบ 3 ปี** ตั้งแต่ปี 2560

ใช้ Social Media

95.3 %

ดูโทรทัศน์/ดูคลิป/ดูหนัง/ฟังเพลงออนไลน์

85.0%

ค้นหาข้อมูล

82.2%

ติดต่อสื่อสารออนไลน์

77.8%

รับ-ส่งอีเมล

69.0%

ซื้อสินค้าออนไลน์

67.3%

อ่านข่าว/บทความ/หนังสืออิเล็กทรอนิกส์ (e-Book)

64.2%

เรียนออนไลน์ (e-Learning)

57.5%

เล่นเกมออนไลน์

56.8%

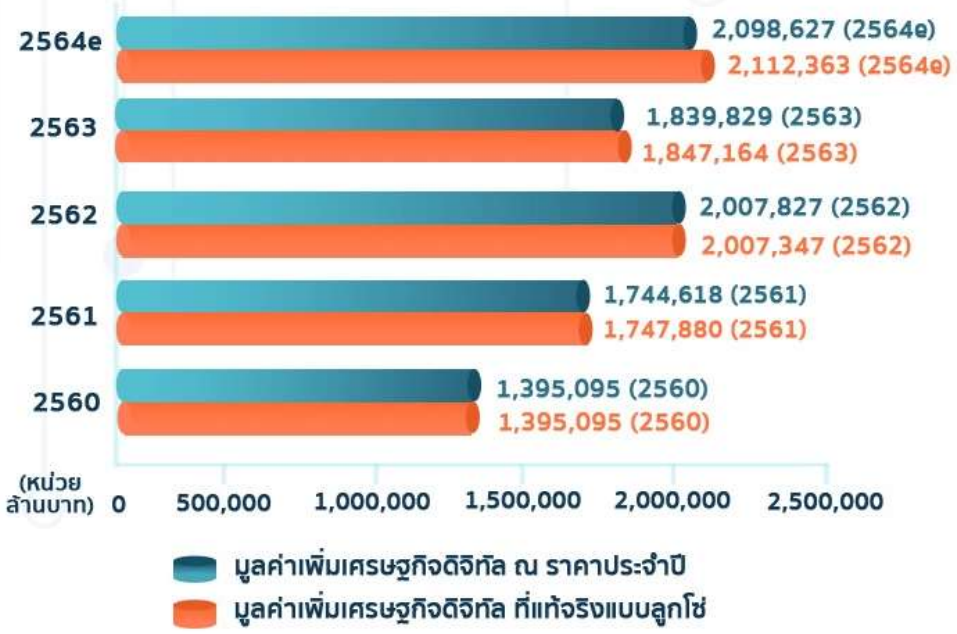
ทำธุรกรรมทางการเงินออนไลน์

56.5%

ETDA | กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | GO DIGITAL with ETDA

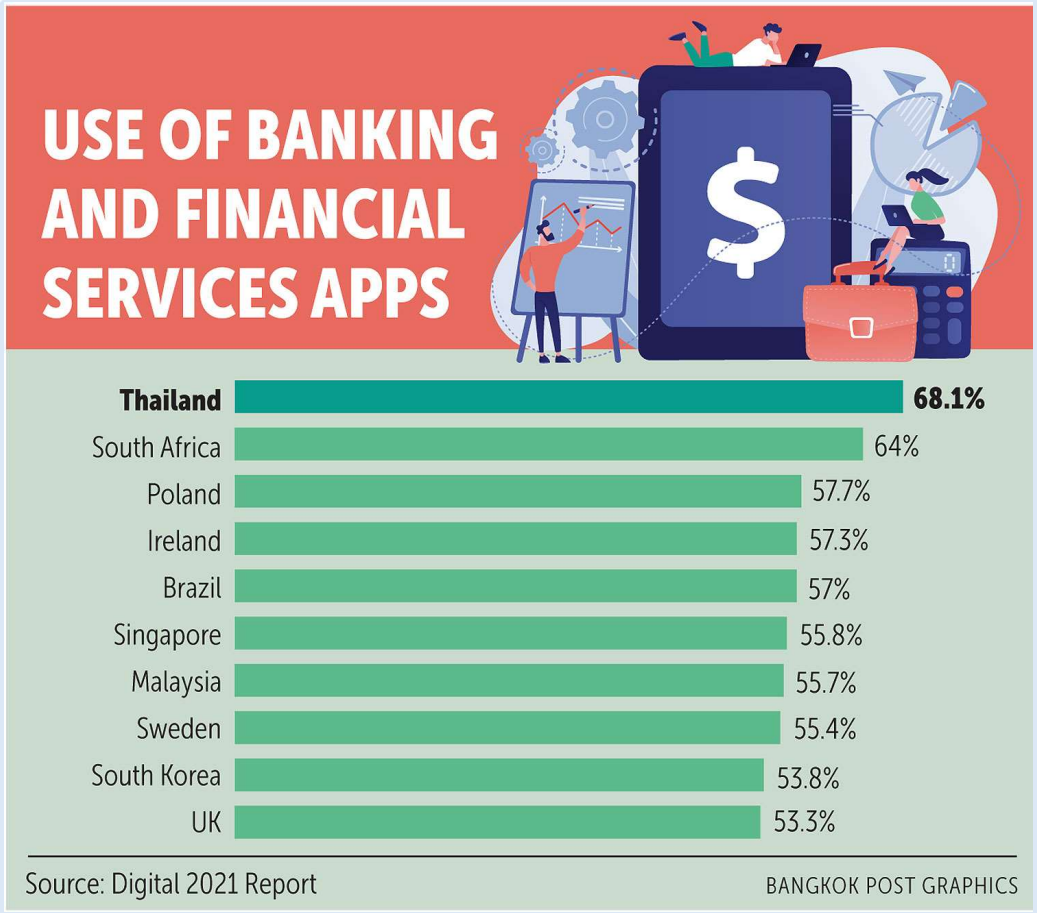
# เศรษฐกิจดิจิทัล ปี 2560 - 2564e

## มูลค่ารวม





ที่มา : https://www.onde.go.th/assets/portals/1/files/1-1.jpg




# ไทยยืนเบอร์ 1

## ใช้งาน Mobile Banking มากที่สุดในโลก ครองแชมป์ 3 สมัยซ้อน

68.1% ของผู้ใช้อินเทอร์เน็ตอายุ 16-64 ปี บอกว่าพวกเขามีการใช้งาน Application ทุกเดือน

Credit: Bangkok Post
Link: https://www.bangkokpost.com/tech/2062199/thai-internet-users-keep-up-top-banking-app-usage-streak

# พ.ร.บ.การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ.2565


# มูลค่าความเสียหายจากอาชญากรรมไซเบอร์

**2015**

**$445 Billion**
**(พันล้าน)**

**2021**

**$2.2 Trillion**
**(ล้านล้าน)** (เพิ่มขึ้น 5 เท่า)

**2025**

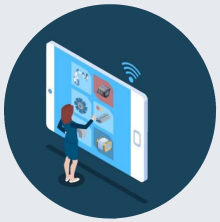

**$10.5 Trillion**
**(ล้านล้าน)**

## 5 อันดับประเภทอุตสาหกรรมที่ถูกโจมตีทางไซเบอร์สูงสุด (%)


1. ภาคการเงินและการธนาคาร
23%

2. ภาคการผลิต
17.7%

3. ภาคพลังงาน
11.1%



4. ภาคการค้าปลีก
10.2%

5. ภาคบริการ
8.7%

Sources: Cybersecurity Ventures, IBM Security 2021

# 2007 Operation Orchard

- หน่วยข่าวกรองของอิสราเอล/สหรัฐ ยืนยันการสร้างโรงงานนิวเคลียร์ในซีเรียที่บริเวณเมือง Al Kibar โดยความช่วยเหลือของเกาหลีเหนือ
- Stealth UAV ถูกส่งเข้าไปปฏิบัติการเพื่อต่อต้านการเตือนของเรดาร์ป้องกันภัยทางอากาศของซีเรีย และเป็นไปได้ว่าระบบคอมพิวเตอร์ควบคุมเรดาร์ที่จัดซื้อจากรัสเซียถูกยึด compromised โดยแฮ็กเกอร์ของอิสราเอล
- เครื่องบินรบ 8 ลำ ประกอบด้วย F-16 และ F-15 พร้อมระเบิด laser-guided 17 ตันและระบบต่อต้านทางอิเล็กทรอนิกส์ เข้าทำลายเป้าหมายที่โรงงานสร้างนิวเคลียร์ได้สำเร็จ โดยไม่มีการต่อต้านทางอากาศ และไม่ปรากฏตัวตนในจอเรดาร์

# Bronze Night 2007

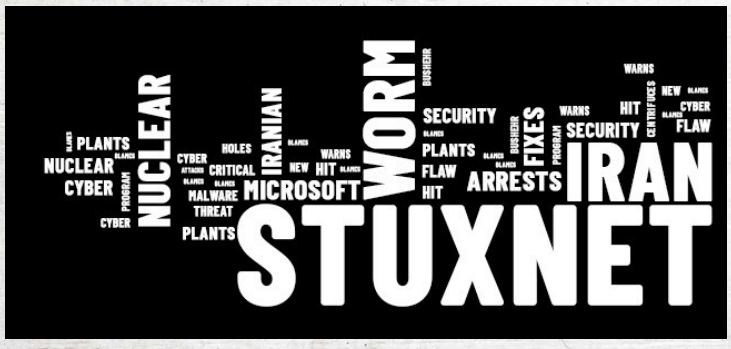
การโจมตี Estonia ด้วย DDoS ที่ใหญ่ที่สุด

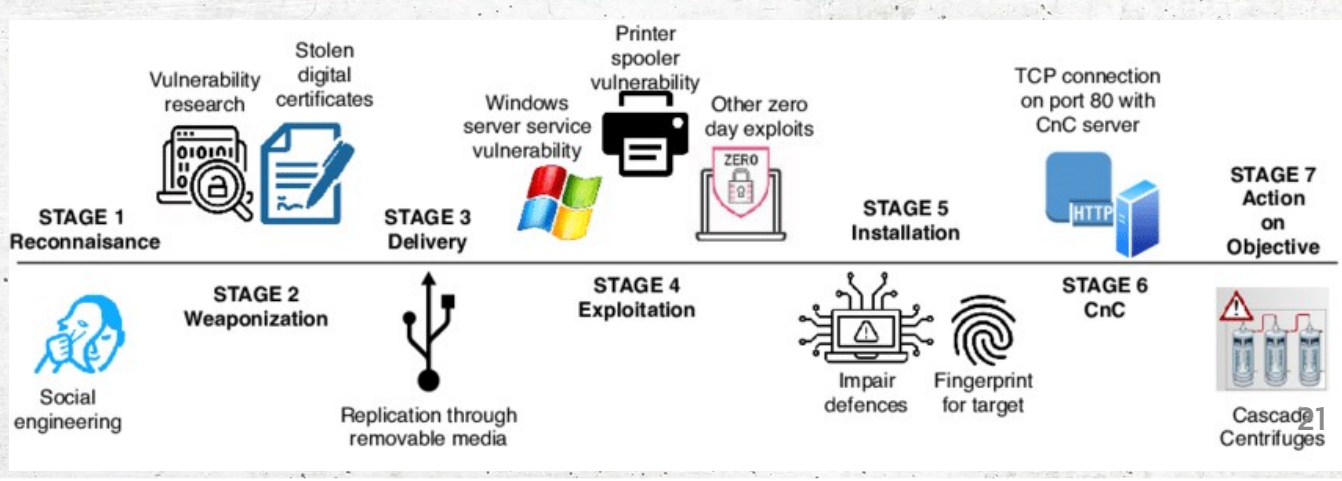
## WWI (Web War One)

- หลังจาก Estonia แยกตัวจากสหภาพโซเวียต มีความขัดแย้งอย่างรุนแรงในประเด็นการย้ายอนุสาวรีย์ในใจกลางเมือง Tallinn ซึ่งสร้างขึ้นมาเพื่อรำลึกถึงทหารรัสเซียที่มาช่วยรบกับกองทัพนาซี
- รัฐบาลจำเป็นต้องย้ายอนุเสาวรีย์เข้าไปในเขตทหารแทน วันรุ่งขึ้นระบบคอมพิวเตอร์ของประเทศทุกระบบทั้งเว็บไซต์ และการให้บริการทางการเงินหยุดชะงักเนื่องจากถูกโจมตีด้วย DDoS (Distributed Denial of Service Attack)
- ระบบต่าง ๆ ไม่สามารถให้บริการได้หลายสัปดาห์

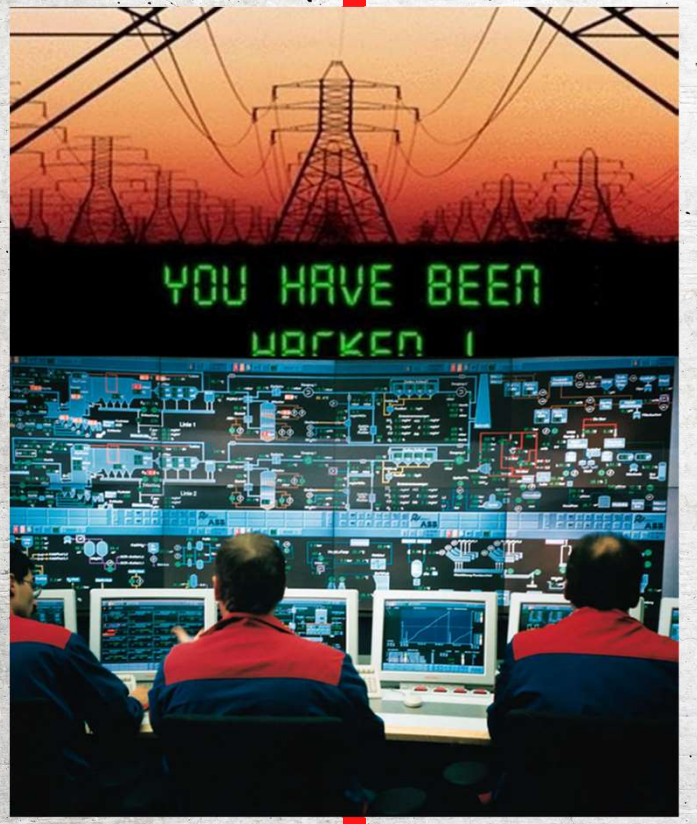
# Stuxnet worm – World first digital weapon 2009

- 2009 Stuxnet worm มัลแวร์พิเศษโจมตีระบบ SCADA – World first digital weapon
- มีการเปิดเผยในปี 2010 ในรายละเอียดเกี่ยวกับ Stuxnet worm แต่คาดว่ามีการใช้มัลแวร์นี้มาตั้งแต่ปี 2005 ระบบ SCADA (Supervisory Control & Acquisition Data) ของโรงงานไฟฟ้านิวเคลียร์ของอิหร่านถูกโจมตีจนไม่สามารถทำงานได้
- นักวิเคราะห์เชื่อว่า Stuxnet worm ถูกพัฒนาตั้งแต่ 2005 โดยอิสราเอล และได้รับความร่วมมือกับสหรัฐฯ



# 2015 UKRAINE POWER GRID CYBER ATTACK




NCSA สกมช

WIRED BACKCHANNEL BUSINESS CULTURE GEAR MORE SUBSCRIBE

KIM ZETTER SECURITY MAR 3, 2016 7:00 AM

## Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.

เป็นที่รู้จักกันว่า First known cyber attack to the power grid แฮ็กเกอร์สามารถเข้ายึดเครื่องคอมพิวเตอร์ที่ใช้ควบคุมระบบไฟฟ้าของทั้ง 3 บริษัทไฟฟ้าของยูเครน ส่งผลให้ไฟฟ้าดับเป็นวงกว้างต่อผู้ใช้ไฟฟ้าประมาณ 250,000 ครัวเรือน เครื่องทำความร้อนที่ใช้ไฟฟ้าไม่สามารถให้ความอบอุ่นได้ในขณะที่อุณภูมิภายนอกต่ำกว่าจุดเยือกแข็ง ระบบน้ำประปาไม่สามารถใช้งานได้ประมาณ 1 ชั่วโมง บริษัทไฟฟ้าส่งเจ้าหน้าที่ออกไปควบคุมสวิทช์แทนการใช้คอมพิวเตอร์ นักวิเคราะห์ระบบพบว่าแฮ็กเกอร์มีความเชื่อมโยงกับคอมพิวเตอร์ในรัสเซีย และหน่วยปฏิบัติการลับของรัสเซีย เนื่องจากความขัดแย้งทางการเมืองระหว่างยูเครนกับรัสเซีย นักวิเคราะห์บางกลุ่มเชื่อว่าการโจมตีครั้งนี้เป็นการทดสอบศักยภาพของปฏิบัติการไซเบอร์ของรัสเซียโดยใช้มัลแวร์ชื่อ BlackEnergy เพื่อเตรียมการโจมตีต่อสหรัฐฯ ในอนาคต

# การโจมตีโรงงานผลิตน้ำประปา Oldsmar ในรัฐ Florida

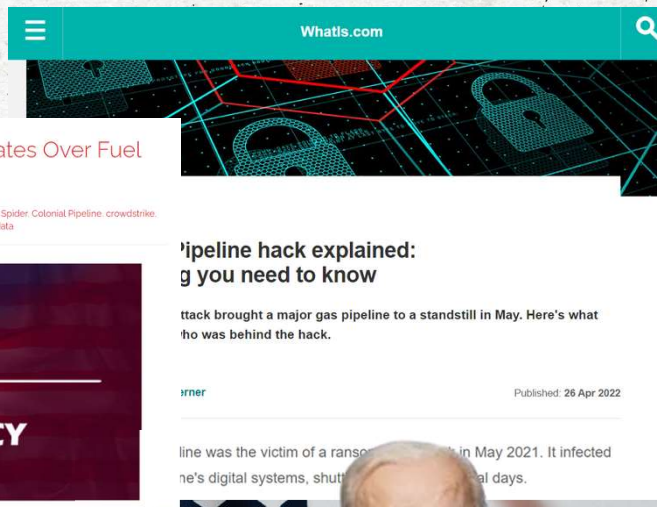

**เมื่อวันที่ 5 กุมพาพันธ์ 2021**
**แฮ็กเกอร์สามารถเข้าถึงระบบบำบัดน้ำได้สำเร็จ ผ่าน remote desktop application TeamViewer**

**โดยแฮ็กเกอร์พยายามเพิ่มระดับโซเดียมไฮดรอกไซด์ในน้ำประปาของเมืองเป็น 100 เท่าของระดับปกติ ซึ่งอาจสร้างพิษให้กับผู้อยู่อาศัยหลายแสนคนที่เป็นผู้ใช้น้ำ**

**อย่างไรก็ตามสถานการณ์ดังกล่าวได้ถูกระงับไว้ได้ทัน เนื่องจากผู้ปฏิบัติงานเฝ้าระวังได้ดูเมาส์ที่เคลื่อนที่ในขณะที่แฮ็กเกอร์เพิ่มระดับได้อย่างทันท่วงที และสามารถแก้ไขนำระบบกลับสู่ระดับปกติได้อย่างรวดเร็ว**

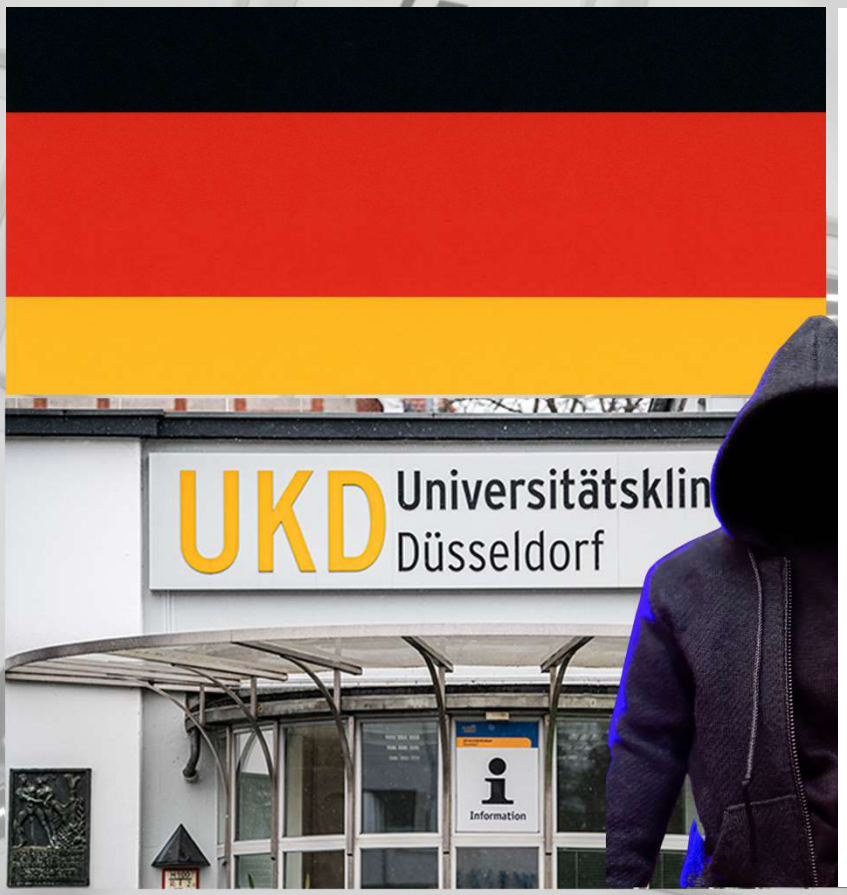

# สหรัฐฯ ประกาศภาวะฉุกเฉินหลัง บ.ท่อส่งน้ำมันรายใหญ่โดนมัลแวร์เรียกค่าไถ่โจมตี




บริษัท โคโลเนียล ไปป์ไลน์ ขนส่งน้ำมันเชื้อเพลิงปริมาณ 2.5 ล้านบาร์เรลต่อวันหรือคิดเป็น 45% ของปริมาณการใช้น้ำมันดีเซล น้ำมันเบนซินและเชื้อเพลิงอากาศยานในฝั่งตะวันออกของสหรัฐฯ แต่ระบบขนส่งน้ำมันของบริษัทต้องหยุดชะงักลงตั้งแต่ 7 พ.ค. 65 เนื่องจากถูกอาชญากรไซเบอร์โจมตีด้วยมัลแวร์เรียกค่าไถ่ เหตุการณ์นี้จะทำให้ราคาน้ำมันสูงขึ้น 2-3% และส่งผลกระทบต่อราคาน้ำมัน


# โรงพยาบาลที่เยอรมันเจอ ransomware จนทำให้ผู้ป่วยเสียชีวิต!




เมื่อวันที่ 10 กันยายน 2020 ระบบเครือข่ายของโรงพยาบาลมหาวิทยาลัย Düsseldorf (University Hospital Düsseldorf - UKD) ในประเทศเยอรมนีได้รับการโจมตีจากแรนซัมแวร์จนไม่สามารถทำการได้ จึงทำให้ผู้ป่วยที่อยู่ในสภาวะฉุกเฉินถูกส่งไปยังโรงพยาบาลอีกแห่งหนึ่งจึงเป็นเหตุทำให้ผู้ป่วยเสียชีวิตลงเนื่องจากได้รับการช่วยเหลือทางการแพทย์ช้าไป จากรายงานของหน่วยงาน Bundesamt für Sicherheit in der Informationstechnik (BSI) ของเยอรมันได้เปิดเผยว่าการโจมตีที่เกิดขึ้นนั้นเกิดจากผู้บุกรุกใช้ประโยชน์จากช่องโหว่ CVE-2019-19781 (Citrix ADC) ซึ่งช่องโหว่นี้ถูกค้นพบและถูกเผยแพร่แล้วตั้งแต่เดือนมกราคม 2020 และได้ทำการออกแพตซ์แก้ไขช่องโหว่แล้วตั้งแต่เดือนมกราคม 2020

หลังจากการโจมตีระบบไอทีของโรงพยาบาลได้หยุดชะงักจึงทำให้ผู้ป่วยที่ต้องการการดูแลฉุกเฉินถูกนำทางไปยังโรงพยาบาลที่ห่างไกลกว่าเพื่อรับการรักษาแทน ซึ่งหลังจากการโจมตีหน่วยงานตำรวจเมือง Düsseldorf ของเยอรมนีได้ทำการติดต่อไปยังผู้ปฏิบัติการที่ทำการโจมตีเรียกค่าไถ่และได้อธิบายว่าเป้าหมายของพวกเขาคือโรงพยาบาลและได้รับผลกระทบอย่างมากจนมีผู้เสียชีวิต ซึ่งหลังผู้ปฏิบัติการ การโจมตีได้รับรู้แล้วจึงส่งมอบคีย์ที่ใช้ในการถอดรหัสจึงทำให้โรงพยาบาลสามารถทำการกู้คืนระบบได้ทั้งนี้เนื่องจากผู้โจมตีใช้ประโยชน์จากช่องโหว่ที่ถูกเปิดเผยซึ่งผู้ดูแลระบบไม่ได้ทำการอัปเดตแพตซ์จึงทำให้เกิดการบุกรุกเครือข่ายได้ ผู้ดูแลระบบควรทำการตรวจสอบระบบและควรทำการแพตซ์อย่างเร่งด่วนเพื่อป้องกันการโจมตีระบบ

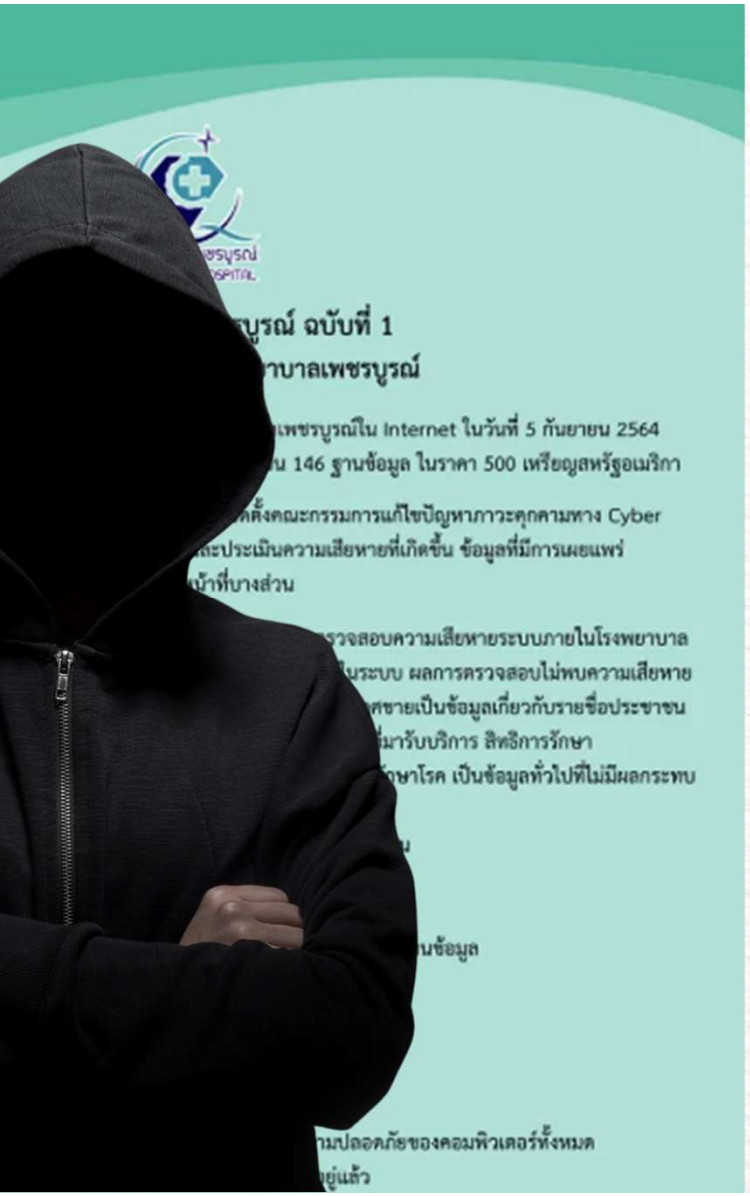
ที่มา: https://www.bleepingcomputer.com/.../ransomware-attack-at-ge.../

# การไฟฟ้าส่วนภูมิภาค (PEA) โดนโจมตี โดยกลุ่ม Maze ransomware


การไฟฟ้าส่วนภูมิภาค (PEA) โดนโจมตีโดยกลุ่ม Maze ransomware June 26, 2020

การไฟฟ้าส่วนภูมิภาค (PEA) ยอมรับว่าโดนไวรัสเรียกค่าไถ่จริง และเร่งแก้ไขอย่างเต็มที่ เมื่อวันที่ 18 มิ.ย. นายธนาเศรษฐ์ พงษ์ทรงเสถียร รองผู้ว่าการสนเทศและสื่อสาร การไฟฟ้าส่วนภูมิภาค (กฟภ.) กล่าวกรณีแอพพลิเคชั่นพีอีเอสมาร์ทพลัส ไม่สามารถใช้งานได้เนื่องจากระบบถูกโจมตีด้วยไวรัสเรียกค่าไถ่ผ่านทางอีเมล

หลังจากนั้นมีรายงานจากทีมวิจัย Cyble ว่ามีข้อมูลจากการไฟฟ้าส่วนภูมิภาคของประเทศไทยถูกเผยแพร่โดยกลุ่ม Maze ransomware โดยข้อมูลที่โดนขโมยออกไปนั้นมีปริมาณมากกว่า 13GB เลยทีเดียว และประกอบข้อมูลเกี่ยวกับ เอกสารการตรวจสอบประจำปี เอกสารการลงทะเบียนขายสินค้า ใบแจ้งหนี้ เป็นต้น




# รพ.เพชรบูรณ์ ขอโทษ ปมโดนแฮกข้อมูลคนไข้ ชี้เป็นข้อมูลทั่วไปไม่มีผลต่อการรักษา

5 กันยายน 2564 มีการประกาศขายข้อมูลคนไข้โรงพยาบาลเพชรบูรณ์ทางอินเทอร์เน็ต **ขนาดข้อมูล 3.75 กิกะไบต์ จำนวน 16 ล้านเรคคอร์ด จาก 146 ฐานข้อมูล ในราคา 500$**

ทางโรงพยาบาลฯ จึงรีบดำเนินการตรวจสอบโดยเร่งด่วน มีการจัดตั้งคณะกรรมการแก้ไขปัญหาภาวะคุกคามทางไซเบอร์ เพื่อตรวจสอบข้อเท็จจริงและประเมินความเสียหายที่เกิดขึ้น ข้อมูลที่มีการเผยแพร่ในอินเทอร์เน็ตแสดงข้อมูลทั่วไปของประชาชนที่มารับบริการและเจ้าหน้าที่บางส่วน ในขั้นต้นมีการปิดกั้นการเข้าถึงอินเทอร์เน็ตจากภายนอก ตรวจสอบความเสียหายระบบภายในโรงพยาบาล มีการตรวจสอบความปลอดภัยด้านไซเบอร์ ตรวจสอบระบบที่ข้อมูลรั่วไม่ให้มีการแฮกข้อมูลอยู่ในระบบ ผลการตรวจสอบไม่พบความเสียหายกับระบบปฏิบัติการที่ใช้ในการดูแลรักษาผู้ป่วย และจากการตรวจสอบขั้นต้น ข้อมูลที่ประกาศขายเป็น**ข้อมูลเกี่ยวกับรายชื่อประชาชนที่มารับบริการโรงพยาบาล ชื่อแพทย์ที่ดูแล และตารางเวรแพทย์ ข้อมูลสัญญาณชีพวันเวลาที่มารับบริการ สิทธิการรักษา เลขประจำตัวผู้ป่วย ไม่ใช่ฐานข้อมูลการรักษา ไม่มีรายละเอียดเกี่ยวกับการวินิจฉัยและรักษาโรค** เป็นข้อมูลทั่วไปที่ไม่มีผลกระทบต่อการดูแลรักษา


เครดิต : MATICHON ONLINE

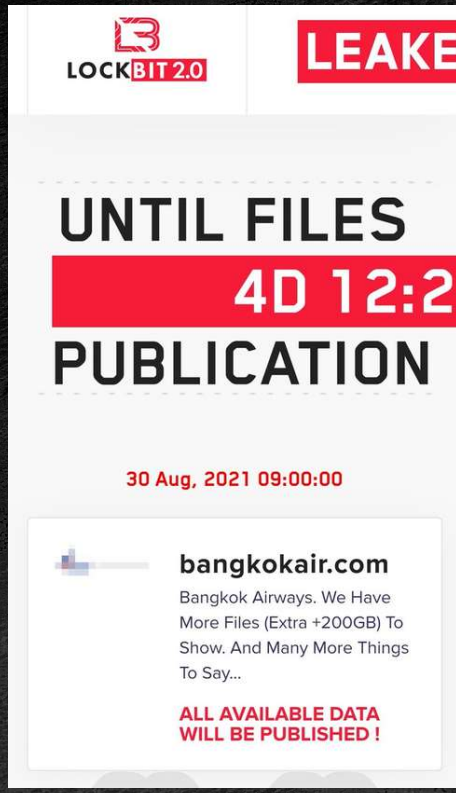
# ข้อมูลหลุด BANGKOK AIRWAYS

# ตกเป็นเหยื่อแฮกเกอร์ โดนเจาะระบบ !!!

# ล้วงข้อมูลส่วนตัว

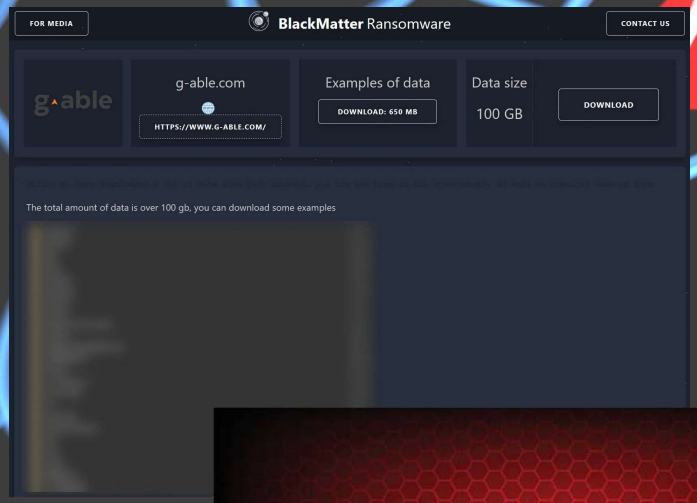

BANGKOK AIRWAYS ออกมาประกาศเมื่อวันที่ 26 สิงหาคม 2564 ที่ผ่านมา ว่าได้พบความผิดปกติในระบบเครือข่ายของบริษัท โดยมีการเข้าถึงระบบสารสนเทศของบริษัทโดยไม่ชอบด้วยกฎหมายและไม่ได้รับอนุญาต ส่งผลให้ข้อมูลผู้ใช้ถูกขโมยไป

ข้อมูลดังกล่าวมีทั้ง ชื่อ นามสกุล สัญชาติ เพศ หมายเลขโทรศัพท์ อีเมล ที่อยู่ ช่องทางการติดต่อสื่อสาร ข้อมูลหนังสือเดินทาง ประวัติการเดินทาง ข้อมูลบัตรเครดิตบางส่วน และข้อมูลอาหารพิเศษของผู้โดยสาร ซึ่งตอนนี้บริษัทได้รายงานเหตุการณ์ดังกล่าวไปยังสำนักงานตำรวจแห่งชาติและหน่วยงานที่เกี่ยวข้องแล้ว
กลุ่มแฮกเกอร์ที่สร้างความปั่นป่วนนี้มีชื่อว่า LockBit เป็นแก๊ง Ransomware ที่ก่อนหน้านี้เตรียมประกาศว่าจะปล่อยข้อมูลลูกค้าของ Bangkok Airway จำนวนกว่า 103 GB ออกสู่สาธารณะในวันที่ 25 สิงหาคมนี้ แต่ล่าสุดเหมือนไม่มีข่าวใด ๆ ตามมา ซึ่งคาดว่า Bangkok Airway น่าจะมีการเจรจากับกลุ่มแฮกเกอร์แล้ว




เครดิต : techhub

# ถูกเรียกค่าไถ่โดยมัลแวร์ BlackMatter ข้อมู
# บางส่วนถูกเผยแพร่





## 25 สิงหาคม 2564 G-ABLE โดน Ransomware จากกลุ่ม BlackMatter โจมตี ส่งผลให้ข้อมูลในระบบถูกเข้ารหัสเพื่อเรียกค่าไถ่ และมีการนำข้อมูลออกมาจากระบบเพื่อเรียกค่าไถ่เพิ่มเติม

### แถลงการณ์อย่างเป็นทางการ

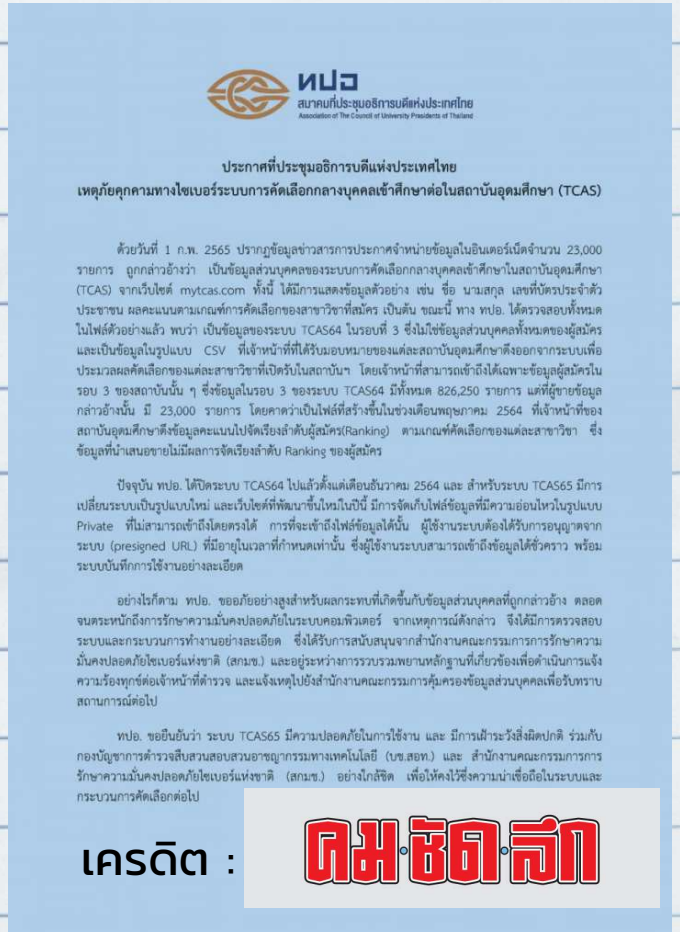
*"จากกรณีที่กลุ่มบริษัทจีเอเบิล ได้ตรวจสอบพบความผิดปกติในระบบเครือข่ายของบริษัทฯ จากมัลแวร์ประเภทหนึ่ง บริษัทฯ ได้ดำเนินการควบคุมเหตุที่เกิดขึ้นทันที พร้อมทั้งตรวจสอบผลกระทบที่เกิดขึ้น โดยได้ทำการกู้คืนระบบที่ได้รับผลกระทบทั้งหมดจากระบบสำรองเป็นที่เรียบร้อย บริษัทฯ ขอยืนยันว่าเหตุการณ์ที่เกิดขึ้นดังกล่าวไม่ส่งผลกระทบต่อการดำเนินงานของบริษัทฯ และไม่ส่งผลกระทบต่อระบบของลูกค้าแต่อย่างใด*

*ทั้งนี้บริษัทฯ ไม่ได้นิ่งนอนใจต่อเหตุการณ์ที่เกิดขึ้น และได้ทำการยกระดับมาตรการป้องกันความปลอดภัยเครือข่ายเป็นขั้นสูงสุด พร้อมทำการตรวจสอบระบบทั้งหมดอย่างละเอียดอีกครั้ง โดยดำเนินการร่วมกับผู้เชี่ยวชาญ 3rdParty ในการทำ Forensic Investigation ต่อไป*

*บริษัทฯ ให้ความสำคัญกับการปกป้องและเก็บรักษาข้อมูลของลูกค้า คู่ค้า และพนักงาน และมุ่งมั่นในการยกระดับระบบคุณภาพสูงสุดเพื่อป้องกันภัยคุกคาม และความเสี่ยงอันอาจจะเกิดขึ้น อย่างไรก็ตามบริษัทฯ จะสื่อสารให้ลูกค้าและผู้ที่เกี่ยวข้องทราบอีกครั้งหากมีข้อมูลเพิ่มเติม"*

เครดิต : Enterprise ITPro

# "ข้อมูลหลุด" ทปอ. ยอมรับข้อมูล TCAS64 ช่วง พ.ค. โดนแฮก จริง 23,000 รายการ !!!!



ทปอ
สภาคณบดีแห่งประเทศไทย
Association of The Council of University Presidents of Thailand

**ประกาศที่ประชุมอธิการบดีแห่งประเทศไทย**
**เหตุภัยคุกคามทางไซเบอร์ระบบการคัดเลือกกลางบุคคลเข้าศึกษาต่อในสถาบันอุดมศึกษา (TCAS)**

ด้วยวันที่ 1 ก.พ. 2565 ปรากฏข้อมูลข่าวสารการประกาศจำหน่ายข้อมูลในอินเตอร์เน็ตจำนวน 23,000 รายการ ถูกกล่าวอ้างว่า เป็นข้อมูลส่วนบุคคลของระบบการคัดเลือกกลางบุคคลเข้าศึกษาในสถาบันอุดมศึกษา (TCAS) จากเว็บไซต์ mytcas.com ทั้งนี้ ได้มีการแสดงข้อมูลตัวอย่าง เช่น ชื่อ นามสกุล เลขที่บัตรประจำตัวประชาชน ผลคะแนนตามเกณฑ์การคัดเลือกของสาขาวิชาที่สมัคร เป็นต้น ซึ่งจากการตรวจสอบทั้งหมดในไฟล์ตัวอย่างแล้ว พบว่า เป็นข้อมูลของระบบ TCAS64 ในรอบที่ 3 ซึ่งไม่ใช่ข้อมูลส่วนบุคคลทั้งหมดของผู้สมัครและเป็นข้อมูลในรูปแบบ CSV ที่เจ้าหน้าที่ที่ได้รับมอบหมายของแต่ละสถาบันอุดมศึกษาดึงออกจากระบบเพื่อประมวลผลคัดเลือกของแต่ละสาขาวิชาที่เปิดรับในสถาบันฯ โดยเจ้าหน้าที่สามารถเข้าถึงได้เฉพาะข้อมูลผู้สมัครในรอบ 3 ของสถาบันนั้น ๆ ซึ่งข้อมูลในรอบ 3 ของระบบ TCAS64 มีทั้งหมด 826,250 รายการ แต่ที่ผู้ขายข้อมูลกล่าวอ้างนั้น มี 23,000 รายการ โดยคาดว่าเป็นไฟล์ที่สร้างขึ้นในช่วงเดือนพฤษภาคม 2564 ที่เจ้าหน้าที่ของสถาบันอุดมศึกษาดึงข้อมูลคะแนนไปจัดเรียงลำดับผู้สมัคร(Ranking) ตามเกณฑ์คัดเลือกของแต่ละสาขาวิชา ซึ่งข้อมูลที่นำเสนอขายไม่มีผลการจัดเรียงลำดับ Ranking ของผู้สมัคร

ปัจจุบัน ทปอ. ได้ปิดระบบ TCAS64 ไปแล้วตั้งแต่เดือนธันวาคม 2564 และ สำหรับระบบ TCAS65 มีการเปลี่ยนระบบเป็นรูปแบบใหม่ และเว็บไซต์ที่พัฒนาขึ้นใหม่ในปีนี้ มีการจัดเก็บไฟล์ข้อมูลที่มีความซ่อนไหวในรูปแบบ Private ที่ไม่สามารถเข้าถึงโดยตรงได้ การที่จะเข้าถึงไฟล์ข้อมูลได้นั้น ผู้ใช้งานระบบต้องได้รับการอนุญาตจากระบบ (presigned URL) ที่มีอายุในเวลาที่กำหนดเท่านั้น ซึ่งผู้ใช้งานระบบสามารถเข้าถึงข้อมูลได้ชั่วคราว พร้อมระบบบันทึกการใช้งานอย่างละเอียด

อย่างไรก็ตาม ทปอ. ขออภัยอย่างสูงสำหรับผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคลที่ถูกกล่าวอ้าง ตลอดจนตระหนักถึงการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ จากเหตุการณ์ดังกล่าว จึงได้มีการตรวจสอบระบบและกระบวนการทำงานอย่างละเอียด ซึ่งได้รับการสนับสนุนจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และอยู่ระหว่างการรวบรวมพยานหลักฐานที่เกี่ยวข้องเพื่อดำเนินการแจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ และแจ้งเหตุไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อรับทราบสถานการณ์ต่อไป

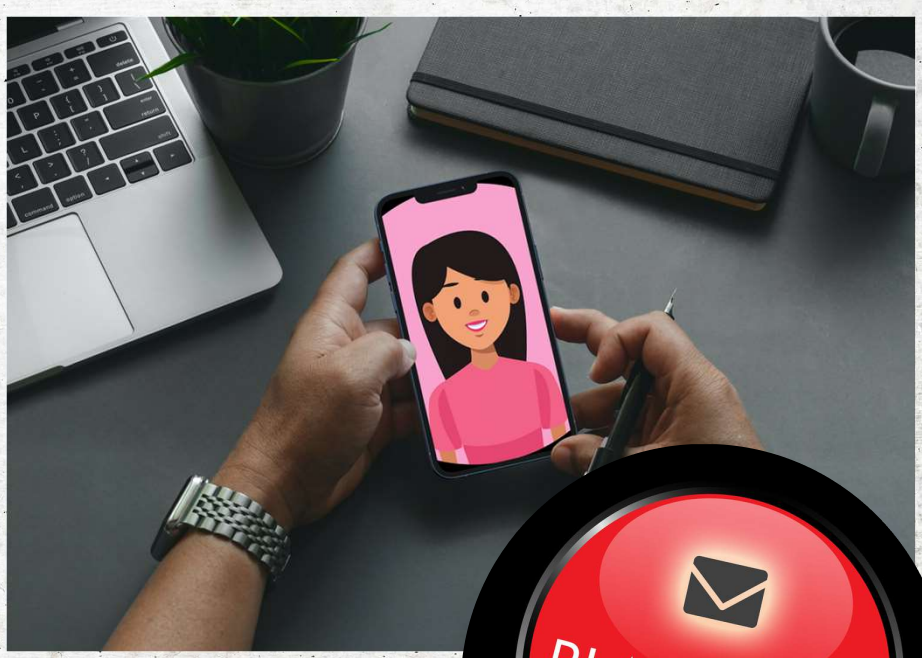
ทปอ. ขอยืนยันว่า ระบบ TCAS65 มีความปลอดภัยในการใช้งาน และ มีการเฝ้าระวังสิ่งผิดปกติ ร่วมกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) อย่างใกล้ชิด เพื่อให้คงไว้ซึ่งความน่าเชื่อถือในระบบและกระบวนการคัดเลือกต่อไป

เครดิต : คมชัดลึก

1 ก.พ. 2565 ปรากฏข้อมูลข่าวสารการประกาศจำหน่ายข้อมูลในอินเทอร์เน็ต จำนวน 23,000 รายการ ถูกกล่าวอ้างว่า เป็นข้อมูลส่วนบุคคลของระบบการคัดเลือกบุคคลเข้าศึกษาในสถาบันอุดมศึกษา (TCAS) จากเว็บไซต์ mytcas.com

ทั้งนี้ ได้มีการแสดงข้อมูลตัวอย่าง เช่น ชื่อ นามสกุล เลขที่บัตรประจำตัวประชาชน ผลคะแนนตามเกณฑ์การคัดเลือกของสาขาวิชาที่สมัคร เป็นต้น

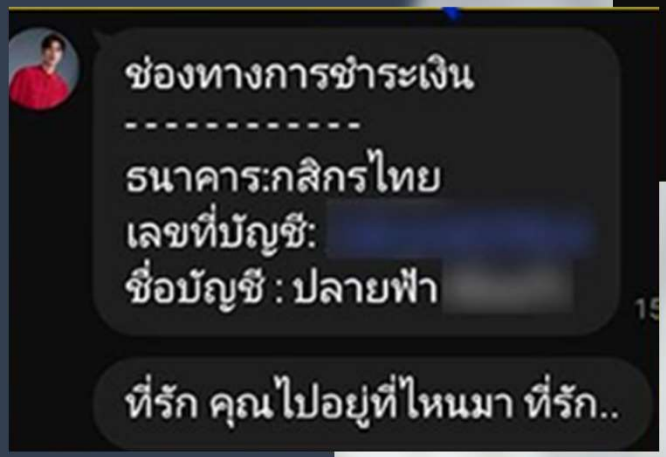

# หนุ่มปลอมโปรไฟล์เป็นสาวหลอก นร.ชาย ม.5 แบล็คเมลเหยื่อเครียดยิงตัวตาย



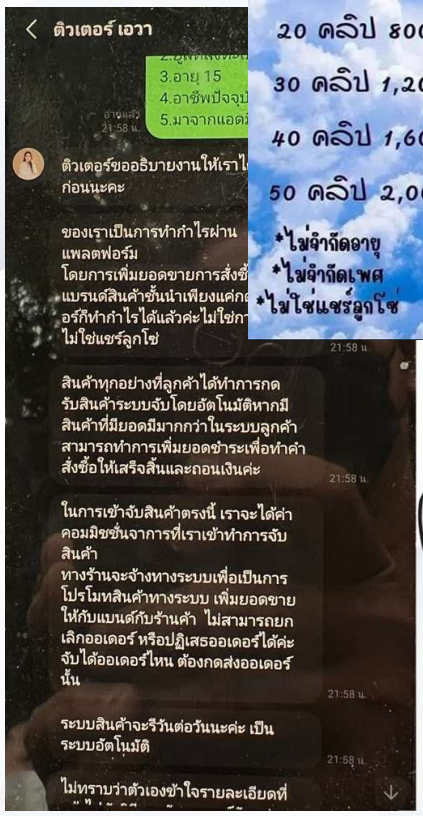

นักเรียนชายชั้น ม.5 โรงเรียนเอกชนชื่อดังในจังหวัดเชียงใหม่ ที่มีอายุเพียง 17 ปี ถูกชายรายหนึ่งปลอมโปรไฟล์ในโซเชียลแอบอ้างเป็นหญิงเข้ามาล่อลวงตีสนิทมาพูดคุย จากนั้นหลอกให้สำเร็จความใคร่ด้วยตัวเองผ่านวิดีโอคอล โดยแอบบันทึกคลิปภาพไว้ จากนั้นนำมาใช้ข่มขู่ให้โอนเงินแลกกับการไม่เปิดเผยคลิปภาพ ทำให้นักเรียนชายรายนี้เครียดอย่างหนัก จนกระทั่งตัดสินใจขโมยอาวุธปืนของพ่อมาใช้ก่อเหตุยิงตัวตายในบ้านพักในพื้นที่อำเภอ สารภี จังหวัดเชียงใหม่ เมื่อคืนวันที่ 15 มี.ค. 65

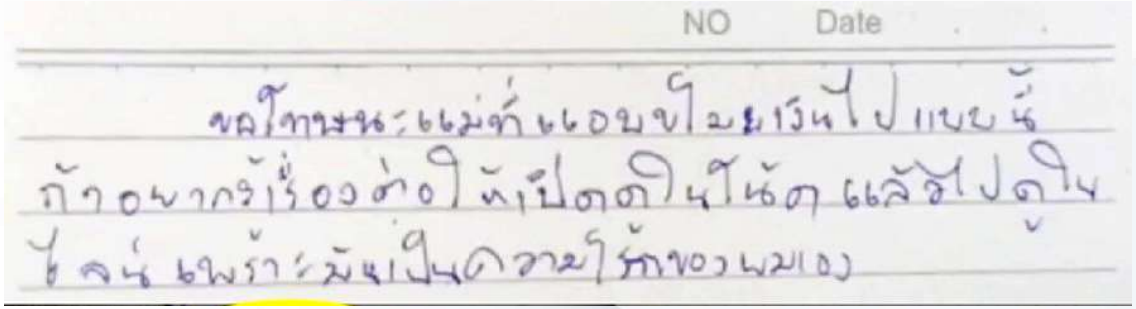
# มิจฉาชีพหลอกใช้รูป "ลี มินโฮ" โอนเงินเกือบแสน

เมื่อวันที่ 29 มิ.ย. 2565 นางสาว เอ สมมุติ อายุ 53 ปี ช่วงประมาณต้นเดือน มิ.ย. 2565 ผู้เสียหายได้โหลดแอปฯหาคู่ มีการพูดคุยกับผู้ใช้งานคนหนึ่ง ตั้งรูปโพรไฟล์เป็นรูป "ลี มิน โฮ" นักแสดงและศิลปินเกาหลีใต้ชื่อดัง ซึ่งเนื้อหาที่มีการพูดคุยกัน ระบุว่าเจ้าตัวชอบผู้เสียหาย และอยากแต่งงานด้วย มิจฉาชีพได้ออกอุบายโดยการถ่ายรูปกระเป๋าแบรนด์เนม และรองเท้าส้นสูงมาให้และจะส่งของมาที่ประเทศไทยพร้อมทั้งโชว์เงินในบัญชีปลอมให้ผู้เสียหายดูก่อนจะหลอกให้เหยื่อโอนเงินเข้าบัญชี


# เด็ก ม.3 ผูกคอดับ ถูกหลอก ดูยูทูป สร้างรายได้


จากเหตุการณ์ นายอาทิตย์ พวงมาลี อายุ 15 ปี นักเรียนชั้น ม.3 ของโรงเรียนแห่งหนึ่งย่านปากเกร็ด ผูกคอตายในป่ารกร้าง โดยเขียนจดหมายระบุสาเหตุว่าถูกกลุ่มมิจฉาชีพให้โอนเงินไปทำยอดซื้อสินค้า ต่อมารู้ตัวว่าถูกหลอก เสียเงินไปเกือบ 15,000 บาท จากบัญชีเงินเก็บของพ่อแม่ จากที่ตรวจสอบข้อมูลในโทรศัพท์มือถือ พบว่าผู้ตายทักข้อความไปติดต่อกับมิจฉาชีพที่โฆษณาหลอกให้ดูยูทูปแล้วจะมีรายได้จากการดู ก่อนจะถูกมิจฉาชีพหลอกให้ไปลงทุนโอนเงินซื้อขายสินค้าแทน จากนั้นได้โอนเงินจากบัญชีไปให้มิจฉาชีพกลุ่มนี้ จำนวน 5 ครั้ง ครั้งแรกกับครั้งที่สองโอนไปรายการละ 100 บาท ครั้งที่สามโอนไป 400 บาท ครั้งที่สี่โอนไป 2,049 บาท และครั้งที่ห้าโอนไป 11,973 บาท รวมเป็นเงินเกือบ 15,000 บาท ในช่วงเวลาตั้งแต่สองทุ่มจนถึงสี่ทุ่มครึ่ง ใช้เวลาแค่สองชั่วโมงครึ่งเท่านั้น ตนเองคิดว่าน้องชายต้องการหาเงินช่วยเหลือพ่อแม่อีกทาง เลยตัดสินใจนำเงินฝากไปลงทุนกับมิจฉาชีพ แล้วเมื่อรู้ว่าถูกหลอกเงินไปจะทำให้พ่อแม่เดือดร้อนไปด้วย จึงตัดสินใจคิดสั้น

# มิจฉาชีพ หลอกให้กลัว และขอให้โอนเงินเพื่อตรวจสอบ

อ้างตัวเป็น ปปง. / ปปส. / อัยการ / DSI / เจ้าหน้าที่รัฐ

คุณโดนออกหมายจับ !

คุณถูกฟ้องดำเนินคดี !

บัญชีรับเงินจากการค้ายาเสพติดหรือคดีฟอกเงิน !

มีหนี้บัตรเครดิต !

บัญชีของคุณถูกอายัด !

บัญชีของคุณถูกล็อคชั่วคราว !

**Gang Call Center**

# ส่องเว็บไซต์หน่วยงานไทยถูกแฮก 5 ครั้ง ใน 5 เดือน ALERT

## แฮกทวิตเตอร์สรรพากร เป็น NFT

16 มกราคม 2565 อยู่ๆ หน้าบัญชีทวิตเตอร์ของกรมสรรพากรก็ถูกเปลี่ยนเป็นรูป ‘ลิงเบื่อ’ พร้อมกับเปลี่ยนชื่อและข้อมูลในบัญชีโดยมีการระบุถึงการซื้อขายทรัพย์สินด้วยเงินดิจิทัลหรือ NFT บนหน้าโปรไฟล์ ทั้งยังลบทวิตเก่าๆ ที่กรมสรรพากรโพสต์ออกไปทั้งหมด

## แฮกเว็บกระทรวงพลังงาน

1 ธันวาคม 2564 เมื่อเข้าสู่หน้าเว็บไซต์ของกระทรวงพลังงานหลายคนก็ต้องงงไป เมื่อข้อมูลที่ปรากฏขึ้นกลายเป็นข้อมูลชักชวนให้ไปเล่นพนันออนไลน์แทน โดยเพจดัง Drama Addict เป็นผู้พบปัญหาและแจ้งให้กับทางกระทรวงพลังงานต่อมา หนึ่งวันทางกระทรวงจึงได้ออกมาแจ้งว่าสามารถแก้ไขและกู้คืนข้อมูลได้เรียบร้อยแล้ว

## แฮกเว็บสำนักงานศาลรัฐธรรมนูญ

11 พฤศจิกายน 2564 เว็บไซต์ของศาลรัฐธรรมนูญถูกแฮกพร้อมอัปโหลดหน้าเว็บไซต์ใหม่ในชื่อ ‘Kangaroo Court’ หรือแสลงคำว่า ‘ศาลเตี้ย’ ในภาษาไทย และอัปโหลดเพลง Guillotine ขึ้นบนหน้าเว็บไซต์ ซึ่งเหตุการณ์นี้เกิดขึ้นหลังศาลรัฐธรรมนูญวินิจฉัยคดีของแกนนำกลุ่มราษฎร นายอานนท์ นำภา, นายภาณุพงศ์ จาดนอก (ไมค์) และ น.ส.ปนัสยา สิทธิจิรวัฒนกุล (รุ้ง)

ซึ่งถูกวินิจฉัยว่าเป็นการใช้สิทธิหรือเสรีภาพเพื่อล้มล้างการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข

## ข้อมูลนักท่องเที่ยวรั่วไหล 106 ล้านคน

22 กันยายน 2564 สื่อต่างชาติรายงานว่าข้อมูลจากบริษัท คอมพาริเทค (Comparitech) บริษัทวิจัยได้สนใจความปลอดภัยทางไซเบอร์จากอังกฤษ พบข้อมูลนักท่องเที่ยวที่เคยเดินทางมาประเทศไทยในรอบ 10 ปีมากกว่า 106 ล้านคนถูกเปิดเผยข้อมูลส่วนตัวเช่น ชื่อ–สกุล หมายเลขพาสปอร์ต วันที่เดินทางเข้าประเทศไทย และอื่นๆ โดยคาดว่าน่าจะมีการรั่วไหลจากสำนักงานตรวจคนเข้าเมือง เนื่องจากมีข้อมูลการเดินทางและเลขพาสปอร์ต และสร้างความกังวลว่าข้อมูลรั่วไหลจะส่งผลกระทบต่อความเชื่อมั่นในการท่องเที่ยว

## ประวัติคนไข้ถูกขาย 16 ล้านราย

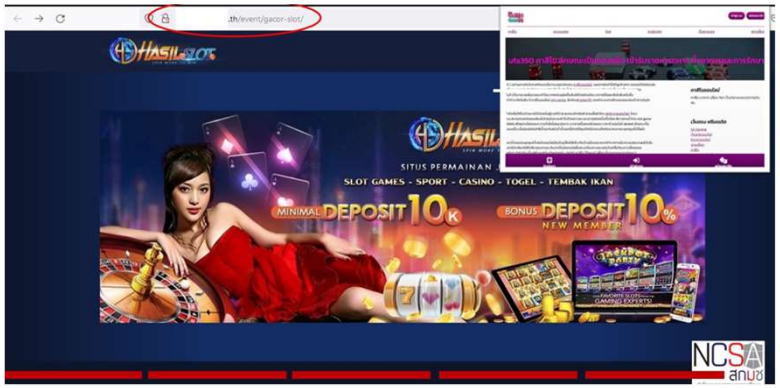
วันที่ 6 กันยายน 2564 ได้มีรายงานข้อมูลพื้นฐานของคนไข้ในระบบสาธารณสุขรั่วไหลกว่า 16 ล้านรายชื่อ โดยมีข้อมูลเช่น ที่อยู่ โทรศัพท์ เลขบัตรประชาชน วันเดือนปีเกิด ชื่อโรงพยาบาล ชื่อบิดา สิทธิในการรักษา และข้อมูลทางการแพทย์ที่รวมถึงชื่อโรงพยาบาลและรหัสทั่วไป โดยมีการลงขายข้อมูลเหล่านี้บนหน้าเว็บไซต์

# ปี 2022 – 2023 ประเทศไทยถูกโจมตีโดยกลุ่ม LOCKBIT จำนวน 20 ครั้ง

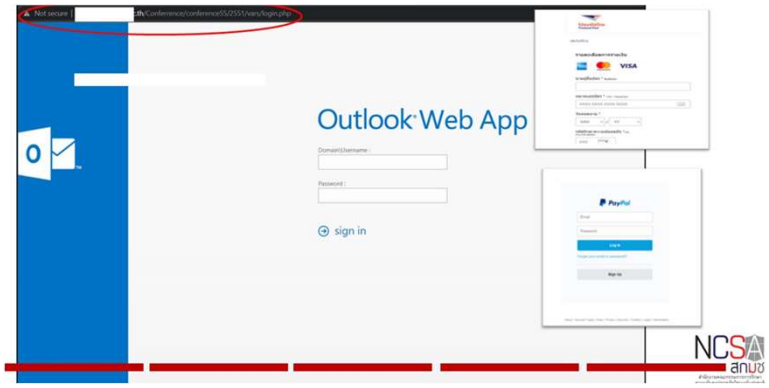

**มูลค่าความเสียหายกว่า**

**800 ล้านบาท**

## Hacked Website (Gambling)

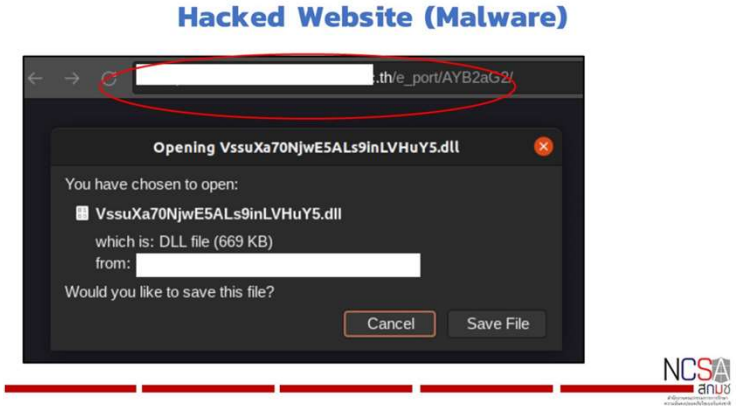



## Website (Phishing)

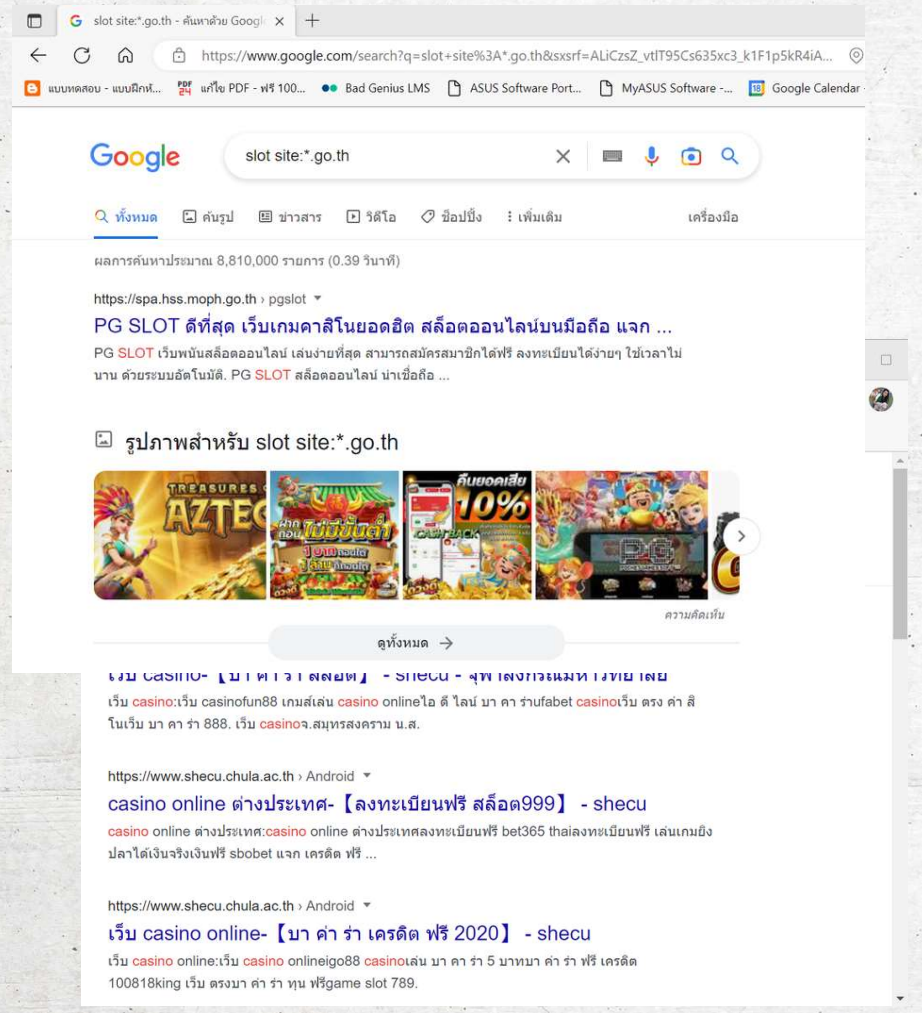



## Hacked Website (Defacement)


## Hacked Website (Malware)



# การฝังโฆษณาเว็บพนันออนไลน์ไว้ในเว็บไซต์ภาครัฐ




สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินการตรวจสอบโดยการค้นหาจากหน้าเว็บไซต์ GOOGLE ในเบื้องต้น โดยใช้คำค้นหาที่สื่อความหมายถึงการพนันออนไลน์จำนวน 3 คำ (Key word) ได้แก่คำว่า casino, slot และ Pgking ซึ่งมีผลการค้นหาที่ตรวจพบเกี่ยวกับการฝังเว็บพนันออนไลน์ในหน่วยงานภาครัฐในประเทศไทย ซึ่งเป็นข้อมูลระหว่างวันที่ 19 - 20 ธันวาคม 2565 รวมทั้งสิ้น ประมาณ 34,072,084 รายการ โดยมีรายละเอียด ดังนี้

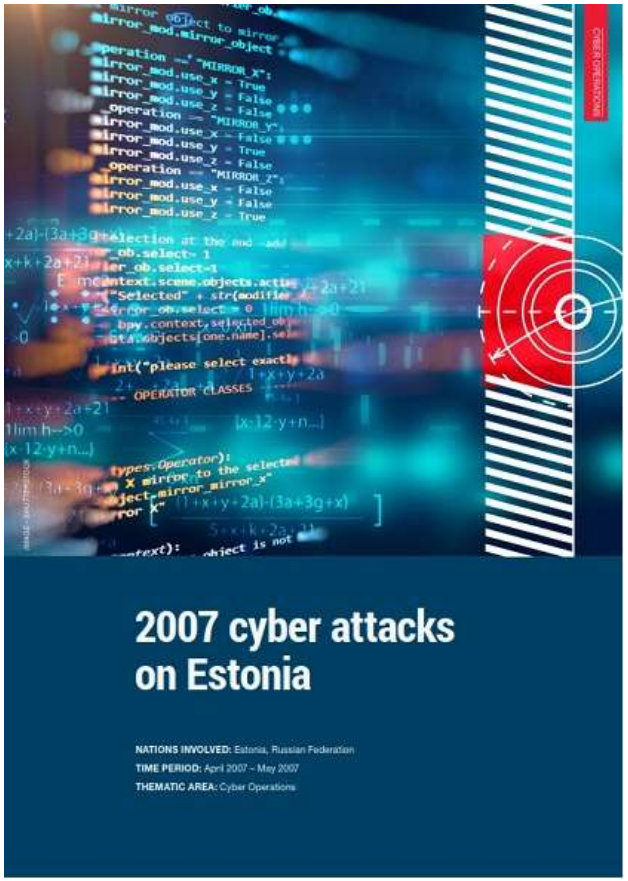
1. คำว่า "casino" โดยใช้คำค้น casino site:*.go.th จำนวน 20 กระทรวง รวม 11,094,557 รายการ
2. คำว่า "slot" โดยใช้คำค้น slot site:*.go.th จำนวน 20 กระทรวง รวมจำนวน 14,858,629 รายการ
3. คำว่า "PGking" โดยใช้คำค้น PGking site:*.go.th จำนวน 13 กระทรวง รวมจำนวน 186,798 รายการ
4. ภายใต้ *.ac.th พบถึง 7,932,100 รายการ


# สรุปสถิติภัยคุกคามทางไซเบอร์
# รวมทั้งสิ้น 26,140,267 เหตุการณ์
## วันที่ 1 ต.ค. 65 – 12 เม.ย. 66

| | |
|---|---|
| Hacked Website (Phishing, Defacement, Gambling, Malware) | 26,139,981 เหตุการณ์ |
| Fake Website | 45 เหตุการณ์ |
| จุดอ่อนช่องโหว่ | 95 เหตุการณ์ |
| Data Breach | 57 เหตุการณ์ |
| Ransomware | 7 เหตุการณ์ |
| อื่นๆ | 82 เหตุการณ์ |

# พรบ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

# 2007 cyber attacks on Estonia




วันที่ 27 เมษายน พ.ศ. 2550
การโจมตีทางไซเบอร์หลายชุดมุ่งเป้าไปที่หน่วยงานรัฐบาลของเอสโตเนีย รวมถึงรัฐสภา เอสโตเนีย ธนาคาร กระทรวง หนังสือพิมพ์ และผู้แพร่ภาพกระจายเสียง ท่ามกลางความไม่ลงรอยกันของประเทศกับรัสเซีย ระบบคอมพิวเตอร์ของประเทศทุกระบบทั้งเว็บไซต์ และการให้บริการทางการเงินหยุดชะงักเนื่องจากถูกโจมตีด้วย DDoS (Distributed Denial of Service Attack) ผลกระทบต่อประชาชนทั่วไปคือการโจมตีแบบปฏิเสธการให้บริการ ไปจนถึงการใช้บ็อตเน็ตสำหรับการกระจายสแปม การสแปมความคิดเห็นของพอร์ทัลข่าวที่ใหญ่กว่าและการทำให้เสื่อมเสียชื่อเสียงรวมถึงเว็บไซต์บริการของหน่วยงานรัฐของเอสโตเนียก็หยุดบริการเช่นกัน

# ภาพรวมกฎหมายดิจิทัล

## POLICY

**กฎหมายการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม**

คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

## FACILITATE & STANDARD

ELECTRONIC TRANSACTION

**กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์**

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เกี่ยวกับอาชญากรรมทางเทคโนโลยี

DIGITAL GOVERNMENT

**กฎหมายรัฐบาลดิจิทัล**

คณะกรรมการรัฐบาลดิจิทัล

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

## SECURE & TRUSTED ENVIRONMENT

POLICY CYBERCRIME

**กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์**

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี - บช.สอท.

DATA PROTECTTION

**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

CYBERSECURITY

**กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์**

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

**หมายเหตุ :** ระดับวิกฤต เป็นอำนาจหน้าที่ สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)

# ความสัมพันธ์กับหน่วยงานไซเบอร์ของประเทศ และกฎหมายที่เกี่ยวข้อง

# SECURE & TRUSTED ENVIRONMENT

❖ **CYBERSECURITY**
**กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์**
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

❖ **CYBERCRIME**
**กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์**
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

❖ **PDPA**
**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- Incident Response
- Critical Information Infrastructure Protection

**หมายเหตุ** : ระดับวิกฤต เป็นอำนาจหน้าที่ สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)

กำหนดความผิดและบทลงโทษ
- ความผิดที่ทำต่อข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยตรง

- ความผิดที่ใช้ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์เป็นเครื่องมือ
- การรวบรวมพยานหลักฐาน และการดำเนินคดี

- รับผิดชอบสืบสวนสอบสวน รวบรวมพยานหลักฐานในคดีที่มีความซับซ้อนหรือเป็นอาชญากรรมทางเทคโนโลยีที่สำคัญ

- มาตรการคุ้มครองข้อมูลส่วนบุคคล
- สิทธิเจ้าของข้อมูล
- ไกล่เกลี่ย ระงับข้อพิพาท

## สาระสำคัญ

**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**
- ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562
- มีผลใช้บังคับ ตั้งแต่วันที่ 28 พฤษภาคม 2562 เป็นต้นไป

**ป้องกัน** → **รับมือ** → **ลดความเสี่ยง**

# พรบ.ไซเบอร์ มีผลบังคับใช้กับใคร ?

## หน่วยงานของรัฐ

ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

## หน่วยงานควบคุมหรือกำกับดูแล

หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนด **ให้มีหน้าที่และอำนาจ**ในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

## หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ : CII

ภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ถูกจัดกลุ่มได้เป็น 8 ประเภท คือ

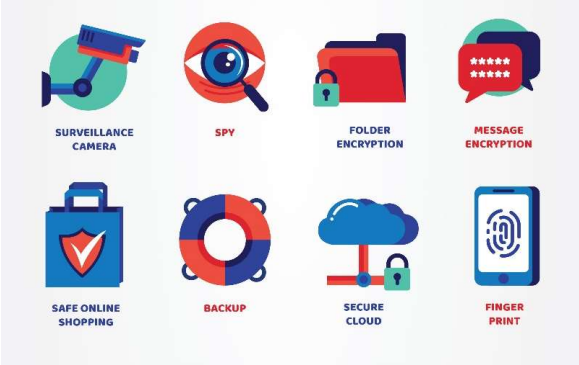
1. ด้านความมั่นคงของรัฐ
2. ด้านบริการภาครัฐที่สำคัญ
3. ด้านการเงินการธนาคาร
4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
5. ด้านการขนส่งและโลจิสติกส์
6. ด้านพลังงานและสาธารณูปโภค
7. ด้านสาธารณสุข
8. หน่วยงานด้านอื่น ตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

# หน่วยงาน CII vs หน่วยงานของรัฐ ตาม พ.ร.บ.ไซเบอร์ 62

| มาตรา | หน่วยงาน CII | หน่วยงานของรัฐ* |
|---|---|---|
| 43 ดำเนินการตามนโยบายและแผนปฏิบัติการฯ | / | / |
| 44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ | / | / |
| 45 มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน | / | / |
| 46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการไปยังสำนักงาน | / | / |
| 52 แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ | / | |
| 53 รับการตรวจสอบมาตรฐานขั้นต่ำจากหน่วยงานควบคุมหรือกำกับดูแล | / | |
| 54 จัดให้มีการประเมินความเสี่ยงฯ รวมทั้งต้องจัดให้มีการตรวจสอบฯ | / | |
| 56 มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ | / | |
| 57 รายงานเหตุภัยคุกคามทางไซเบอร์ และปฏิบัติตามส่วนที่ 4 | / | |
| 58 ตรวจสอบ ประเมิน ป้องกัน รับมือ ลดความเสี่ยง ตามประมวลฯ และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว | / | / |

*หมายถึง หน่วยงานของรัฐที่มิได้เป็นหน่วยงาน CII

# สาระสำคัญ




## หลักการสำคัญของพระราชบัญญัติ

ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ (เช่น ไวรัส หรือมัลแวร์) ที่จะทำให้เกิดผลกระทบต่อภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งหน่วยงานของรัฐและหน่วยงานเอกชน

ให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง

ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ


รวมจำนวน 83 มาตรา

## บททั่วไป
(วันบังคับใช้/นิยาม/ผู้รักษาการ)

## หมวด 1
## คณะกรรมการ

กมช.
นรม. เป็นประธาน ฯ

กกม.
รมว.ดศ.
เป็นประธานฯ

คณะกรรมการ 3 คน ดำเนินการรับมือภัยที่เร่งด่วนได้ทันที

หมวด 3
## การรักษาความมั่นคงปลอดภัยไซเบอร์

- ส่วนที่ 1 นโยบายและแผน
- ส่วนที่ 2 การบริหารจัดการ
- ส่วนที่ 3 โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ส่วนที่ 4 การรับมือภัยคุกคามทางไซเบอร์

## บทเฉพาะกาล

## หมวด 2
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

## หมวด 4
บทกำหนดโทษ

# คำนิยามที่สำคัญ

- **“ภัยคุกคามทางไซเบอร์”**

หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

- **“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”**

หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชน ใช้ในกิจการของตน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

- **“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”**

หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- **“หน่วยงานของรัฐ”**

หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

# ระดับของภัยคุกคามทางไซเบอร์

**สภาความมั่นคงแห่งชาติ**

**กมช. อาจมอบหมายให้เลขาฯ ดำเนินการ ได้ทันทีเท่าที่จำเป็น**
เพื่อเยียวยาความเสียหาล่วงหน้าโดยไม่ต้องขอศาล และต้องรายงานต่อศาลคู่ขนานไป

## ระดับ วิกฤต

- การโจมตีระบบ CII ระดับสูงขึ้นส่ง**ผลกระทบรุนแรงเป็นวงกว้างทำให้การบริการล้มเหลวทั้งระบบ /ไม่สามารถแก้ไข**ด้วยมาตรการเยียวยาตามปกติ
- **มีความเสี่ยงที่จะลุกลามไปยัง CII อื่นๆ** อาจทำให้คนจำนวนมากเสียชีวิต/**ระบบถูกทำลายเป็นวงกว้าง**ระดับประเทศ
- **กระทบต่อความสงบเรียบร้อย**ของประชาชน/เป็นภัยต่อความมั่นคงต่อรัฐอาจทำให้ประเทศอยู่ในภาวะคับขัน
- **มีการกระทำความผิดเกี่ยวกับการก่อการร้าย**จำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข เอกราช ผลประโยชน์ของชาติ การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อย
- การแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

## ระดับ ร้ายแรง

- **การโจมตีเพิ่มขึ้น**อย่างมีนัยสำคัญ
- มีความเสียหายต่อ**ระบบ CII จนไม่ทำงาน** /ความมั่นคงของรัฐ/ความสัมพันธ์ระหว่างประเทศ/การป้องกันประเทศ/เศรษฐกิจ/การสาธารณสุข/ความปลอดภัยสาธารณะ/ความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้
- การดำเนินการที่กระทบสิทธิต้องขอคำสั่งศาล/สามารถอุทธรณ์ได้ตามกระบวนการปกติของศาล


## ระดับ ไม่ร้ายแรง

- **มีความเสี่ยงอย่างมีนัยสำคัญ**ทำให้ระบบ CII/บริการของรัฐ**ด้อยประสิทธิภาพลง**
- ผู้ได้รับคำสั่งที่เกี่ยวข้องสามารถอุทธรณ์ได้

# กลไกการบริหารจัดการด้านไซเบอร์ตาม พ.ร.บ.ไซเบอร์ 62

1

**มาตรา 9**

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

**มาตรา 12**

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

**มาตรา 25**

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

**มาตรา 22 วรรคสอง**

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ("National CERT")

**มาตรา 9(8)**

หน่วยงานควบคุมหรือกำกับดูแล

2

**มาตรา 50**

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงาน CII หรือ "Sectoral CERT"

3

**มาตรา 49**


หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Critical Information Infrastructure (CII)

4

# คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

## หน้าที่และอำนาจ

- กำหนดนโยบาย
- กำหนดแผนปฏิบัติการ
- กำหนดมาตรการ แนวทาง และประกาศหลักเกณฑ์ต่างๆ

รองนายกรัฐมนตรี
ปฏิบัติหน้าที่ประธานกรรมการ

**กรรมการโดยตำแหน่ง**

- รัฐมนตรีช่วยว่าการกระทรวงกลาโหม
- รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- ปลัดกระทรวงการคลัง
- ปลัดกระทรวงยุติธรรม
- ผู้บัญชาการตำรวจแห่งชาติ
- เลขาธิการสภาความมั่นคงแห่งชาติ

**กรรมการผู้ทรงคุณวุฒิ**

- ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- ด้านวิศวกรรมศาสตร์
- ด้านกฎหมาย
- ด้านการเงิน
- ด้านสาธารณสุข
- ด้านความสัมพันธ์ระหว่างประเทศ

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ

เมื่อวันที่ ๒๐ ธ.ค. ๖๕

# คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

## หน้าที่และอำนาจ

- กำกับดูแล National CERT
- กำหนดประมวลแนวทางปฏิบัติ และมาตรฐานหน้าที่ CII
- บริหารจัดการเหตุการณ์ภัยคุกคามทางไซเบอร์

รัฐมนตรีว่าการกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ประธานกรรมการ

**กรรมการโดยตำแหน่ง**

- ปลัดกระทรวงการต่างประเทศ
- ปลัดกระทรวงคมนาคม
- ปลัดกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม
- ปลัดกระทรวงพลังงาน
- ปลัดกระทรวงมหาดไทย
- ปลัดกระทรวงสาธารณสุข
- ผู้บัญชาการตำรวจแห่งชาติ
- ผู้บัญชาการทหารสูงสุด
- เลขาธิการสภาความมั่นคงแห่งชาติ
- ผู้อำนวยการสำนักข่าวกรองแห่งชาติ
- ผู้ว่าการธนาคารแห่งประเทศไทย
- เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์ และตลาดหลักทรัพย์
- เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

**กรรมการผู้ทรงคุณวุฒิ**

- ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- ด้านวิทยาศาสตร์หรือด้านวิศวกรรมศาสตร์
- ด้านกฎหมาย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กรรมการและเลขานุการ

เมื่อวันที่ ๒๐ ธ.ค. ๖๕

# คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

## หน้าที่และอำนาจ

- กำหนดนโยบาย ทิศทาง และบริหารจัดการ สกมช.
- ออกข้อบังคับ / ควบคุมการบริหารงาน
- อนุมัติการใช้จ่ายเงิน งบประมาณ
- ควบคุมการบริหารงานและการดำเนินงาน ของสำนักงานและเลขาธิการ


เมื่อวันที่ ๒๐ ธ.ค. ๖๕

# สรุปหน้าที่ของคณะกรรมการที่สำคัญ ตาม พ.ร.บ.ไซเบอร์ 62

## 1 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

ส่งเสริม/พัฒนาขีดความสามารถ
9(1) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
9(3) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
9(5) มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
9(6) กรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศ

กำกับดูแล
9(2) นโยบายการบริหารจัดการฯ
9(4) มาตรฐานและแนวทาง รวมถึงมาตรฐานขั้นต่ำ
9(8) ข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ
49 หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ
50 ลักษณะหน้าที่และความรับผิดชอบของ Sectoral CERT

## 1 คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

กำกับดูแล
13(4) ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
13(5) หน้าที่ของหน่วยงาน CII และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล
13(6) ระดับของภัยคุกคามทางไซเบอร์

# สรุปหน้าที่ของหน่วยงานที่เกี่ยวข้องตาม พ.ร.บ.ไซเบอร์ 62

## 2 หน่วยงาน Regulator

**กำกับดูแล**
13(5) กำหนดมาตรฐานที่เหมาะสม
9(8), 49 กำหนดเกณฑ์รอง, รายงาน
53 ตรวจสอบมาตรฐานขั้นต่ำ
54 ตรวจสอบความมั่นคงปลอดภัย

**ป้องกัน**
43 ดำเนินการตามนโยบายและแผน
44-45 ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
46 แจ้งรายชื่อบริหารและปฏิบัติการไปยัง สกมช.
52 รับแจ้งรายชื่อและข้อมูลติดต่อจาก CII

**รับมือ**
57-58 รับแจ้งเหตุภัยคุกคามทางไซเบอร์
59 ร่วมกับ Sectoral CERT รวบรวม ข้อมูล ตรวจสอบ ... ช่วยเหลือ CII

## 3 Sectoral CERT

**รับมือ**
50 ลักษณะ หน้าที่และความรับผิดชอบของ Sectoral CERT
52 รับแจ้งรายชื่อและข้อมูลติดต่อฯ จาก CII
59 ร่วมกับ Reg รวบรวมข้อมูล ตรวจสอบ ... ช่วยเหลือ CII

## 4 หน่วยงาน CII

**ป้องกัน**
43 ดำเนินการตามนโยบายและแผน
44-45 ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
46 แจ้งรายชื่อบริหารและปฏิบัติการไปยัง สกมช.
54 ประเมินความเสี่ยง และตรวจสอบ

**(ต่อ)**
52 แจ้งรายชื่อและข้อมูลติดต่อเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ดูแลระบบ ไปยัง สกมช., Reg, Sectoral CERT

**รับมือ**
56 กลไกหรือขั้นตอนเพื่อการเฝ้าระวัง
57 รายงานเหตุต่อ สกมช. และ Reg
58 ป้องกัน รับมือ ลดความเสี่ยง

# อำนาจหน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

หมวด ๒
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๒๐ ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

มาตรา ๒๑ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

มาตรา ๒๒ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ และ กกม. และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

- เสนอแนะและสนับสนุนในการจัดทำนโยบาย แผน และแผนปฏิบัติการ
- เสริมสร้างความรู้ความเข้าใจ สร้างความตระหนักด้านภัยคุกคามทางไซเบอร์
- จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- เป็นศูนย์กลางในการรวบรวม และวิเคราะห์ข้อมูล รวมทั้งเผยแพร่ข้อมูล
- ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน CII
- ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศ
- ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานฯ ในประเทศและต่างประเทศ
- ศึกษาและวิจัยข้อมูลที่จำเป็นเพื่อจัดทำข้อเสนอแนะ
- ดำเนินการและประสานงานกับหน่วยงานในการตอบสนองและรับมือกับภัยคุกคาม
- ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ ตลอดจนดำเนินการฝึกอบรม
- เฝ้าระวังความเสี่ยง ติดตาม วิเคราะห์ ประมวลผล และการแจ้งเตือน

# Positioning


**คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)**

**กระทรวงกลาโหม (กห.)**

**กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.)**

ป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

| ด้านความมั่นคงของรัฐ | ด้านบริการภาครัฐที่สำคัญ | ด้านการเงินการธนาคาร | ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม | ด้านการขนส่งและโลจิสติกส์ | ด้านพลังงานและสาธารณูปโภค | ด้านสาธารณสุข |
|---|---|---|---|---|---|---|
| สำนักงานปลัดกระทรวงกลาโหม | กระทรวงการคลัง | ธนาคารแห่งประเทศไทย | สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ | สำนักงานตำรวจแห่งชาติ | กระทรวงพลังงาน | สำนักงานปลัดกระทรวงสาธารณสุข |
| สำนักงานตำรวจแห่งชาติ | กรมศุลกากร | สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ | | กรมการขนส่งทางราง | การประปาส่วนภูมิภาค (เฉพาะบริการส่วนภูมิภาค) | สำนักงานคณะกรรมการอาหารและยา |
| สำนักงานสภาความมั่นคงแห่งชาติ | กรมการปกครอง กรมชลประทาน | | | สำนักงานปลัดกระทรวงคมนาคม | | สำนักงานปรมาณูเพื่อสันติ |
| | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) | | | สำนักงานการบินพลเรือนแห่งประเทศไทย | | |

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีภารกิจด้านบริการสำคัญของชาติ หรือนโยบายของภาครัฐ หากเกิดภัยคุกคามจะส่งผลกระทบต่อความมั่นคงของประชาชน มี 7 ลักษณะหน่วยงาน โดยมีหน่วยงานกำกับดูแล (Regulator) 19 หน่วยงาน

# การจัดตั้ง Sectoral CERT

**ฐานอำนาจ**

**พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

**มาตรา 50** ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ 1/2564 เมื่อวันที่ 25 มิถุนายน 2564 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังนี้


**ข้อ (3)** ให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในแต่ละด้านจัดตั้งหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยหน่วยงานควบคุมหรือกำกับดูแลอาจจัดให้มีหลักเกณฑ์ เงื่อนไขและแนวทางในการพิจารณา คุณสมบัติ และความเหมาะสมของการเป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามวรรคหนึ่ง มีลักษณะ หน้าที่และความรับผิดชอบ รวมถึงจัดให้มีการดำเนินภารกิจหรือให้บริการไม่น้อยกว่าหลักเกณฑ์ที่กำหนดแนบท้ายประกาศฉบับนี้


## หน่วยงานที่ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

### 1 สำนักงานสภาความมั่นคงแห่งชาติ

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านความมั่นคงของรัฐ รับหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านความมั่นคงของรัฐฝ่ายพลเรือน (Thailand Civilian Sector CERT (TCS-CERT) เรียบร้อยแล้ว

### 2 สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.)

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านการเงินการธนาคาร ได้ดำเนินการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน เรียกว่า TCM-CERT เรียบร้อยแล้ว

### 3 สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.)

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านบริการภาครัฐที่สำคัญ ได้ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐที่สำคัญ ที่มีการให้บริการโดยตรงแก่ประชาชน โดยมีหน่วยงานที่อยู่ภายในการดูแลของศูนย์ประสานฯ ประกอบด้วย **(สพร. , สำนักงานตรวจคนเข้าเมือง และ กรมป้องกันและบรรเทาสาธารณภัย)** และทั้ง 3 หน่วยงาน ได้รับการตอบรับเข้าร่วมการจัดตั้งศูนย์ฯ แล้ว เรียบร้อยแล้ว


## หน่วยงานที่ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

**4** **สำนักงานปลัดกระทรวงกลาโหม**

เป็นหน่วยงานควบคุมหรือกำกับดูแล ด้านความมั่นคงของรัฐ แจ้งว่า ได้ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (Ministry of Defense Computer Security Incident Response Team : MODCSIRT) เรียบร้อยแล้ว

**5** **สำนักงานปลัดกระทรวงสาธารณสุข**

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านสาธารณสุข แจ้งว่า ได้ดำเนินการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เรียบร้อยแล้ว

**6** **สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.)**

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านเทคโนโลยีสารสนเทศและโทรคมนาคม แจ้งให้ทราบว่า กสทช. ได้ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม เรียกว่า TTC-CERT เรียบร้อยแล้ว


## หน่วยงานที่ดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

7

### ธนาคารแห่งประเทศไทย (ธปท.)

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านการเงินการธนาคาร ธปท. มีศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT (TB-CERT) ทำหน้าที่ประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ภาคการธนาคาร ตลอดจนมีหน้าที่ในการช่วยเหลือ สนับสนุน **หรือปฏิบัติงานร่วมกับ สกมช.** เรียบร้อยแล้ว

8

### สำนักงานปลัดกระทรวงพลังงาน

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านพลังงาน แจ้งว่า ได้ดำเนินการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านพลังงาน (Energy CERT) เรียบร้อยแล้ว

# หน่วยงานที่อยู่ระหว่างดำเนินการจัดตั้ง Sectoral CERT

## สำนักงานปลัดกระทรวงคมนาคม

เป็นหน่วยงานควบคุมหรือกำกับดูแล ด้านการขนส่งและโลจิสติกส์ บริการขนส่งทางน้ำ แจ้งว่าอยู่ระหว่างดำเนินการในเบื้องต้น โดยได้แต่งตั้งคณะทำงานดำเนินงานรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการขนส่งและโลจิสติกส์ ที่มีภารกิจหรือบริการขนส่งทางน้ำ เพื่อดำเนินการเกี่ยวกับการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์

## สำนักงานการบินพลเรือนแห่งประเทศไทย

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านการขนส่งและโลจิสติกส์ บริการขนส่งทางอากาศ แจ้งว่า อยู่ระหว่างขั้นตอนการดำเนินการจัดตั้งศูนย์ฯ ซึ่งมีการแต่งตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน CII ที่มีภารกิจหรือให้บริการขนส่งทางอากาศ โดยมีผู้แทนจากหน่วยงานที่เกี่ยวข้องเข้าร่วมเป็นคณะกรรมการฯ และมีช่องทางสำหรับการติดต่อสื่อสารเป็นกลุ่ม LINE Open chat สำหรับแจ้งเหตุภัยคุกคามทางไซเบอร์เบื้องต้น

# หน่วยงานที่อยู่ระหว่างดำเนินการจัดตั้ง Sectoral CERT

## กรมการปกครอง

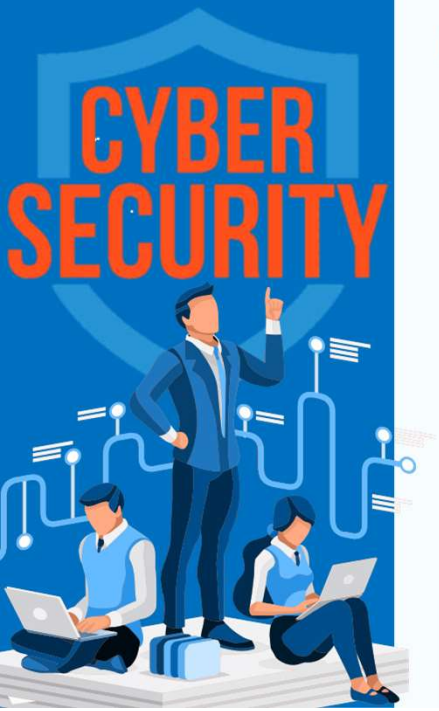
เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านบริการภาครัฐที่สำคัญ แจ้งว่า อยู่ในระหว่างขั้นตอนดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยได้มีการประสานกับหน่วยงานภายในที่เกี่ยวข้อง เพื่อจัดทำแนวทางการดำเนินการร่วมกัน และแต่งตั้งผู้ที่เกี่ยวข้องเข้าเป็นคณะทำงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ ต่อไป

## สำนักงานตำรวจแห่งชาติ

เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านความมั่นคงของรัฐ โดยที่ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บก.สอท.) ในฐานะหน่วยงานที่ได้รับมอบหมายจากสำนักงานตำรวจแห่งชาติ ได้แจ้งว่า ขณะนี้ได้ดำเนินการจัดทำร่างประมวลแนวทางปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ สำนักงานตำรวจแห่งชาติ ฉบับที่ 1 เพื่อเป็นนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานตำรวจแห่งชาติ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 โดยเสนอผ่านคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสำนักงานตำรวจแห่งชาติ (DCIO ตร.) พิจารณา/ตรวจสอบ/ปรับปรุง/แก้ไข และให้ความเห็นร่างฯ ดังกล่าว ซึ่งหากผ่านเห็นชอบจากคณะกรรมการฯ แล้ว จะดำเนินการตามกระบวนการขั้นตอนการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสำนักงานตำรวจแห่งชาติ (CERT) ต่อไป


65

## ประชาชนได้อะไรจาก พ.ร.บ. ไซเบอร์




1 ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญ มีความปลอดภัยสามารถให้บริการได้อย่างต่อเนื่อง


2 มีแนวทางในการรับมือภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบเป็นวงกว้างและกลับมาทำงานได้อย่างรวดเร็ว

3 มีการจัดตั้งหน่วยงานขึ้นมาดูแลมาตรฐานด้านความปลอดภัยไซเบอร์และให้ความช่วยเหลือแก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญ

4 เมื่อเกิดภัยคุกคามร้ายแรง การเข้าไปแก้ไขปัญหาที่ต้องเข้าถึงทรัพย์สินจะต้องใช้คำสั่งศาลเพื่อคุ้มครองสิทธิ์

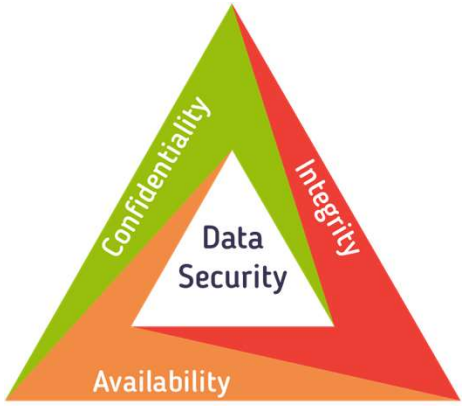
# คำถาม

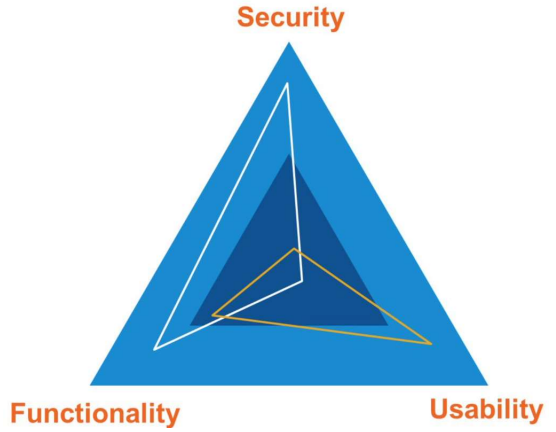
## พระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2562 หน่วยงานใด เป็นผู้ต้องปฏิบัติตาม พรบ.

# การ Implement Cyber Security for University


GAME OVER
GAME OVER
CONTRA
สูตรสำเร็จ เพื่อ 30 Lives
B
A
START

# เคล็ดลับสู่ความสำเร็จ เพื่อ Cybersecurity

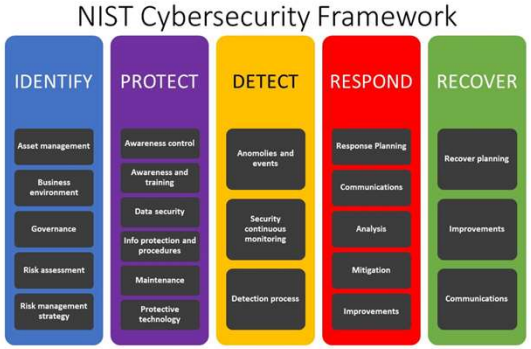


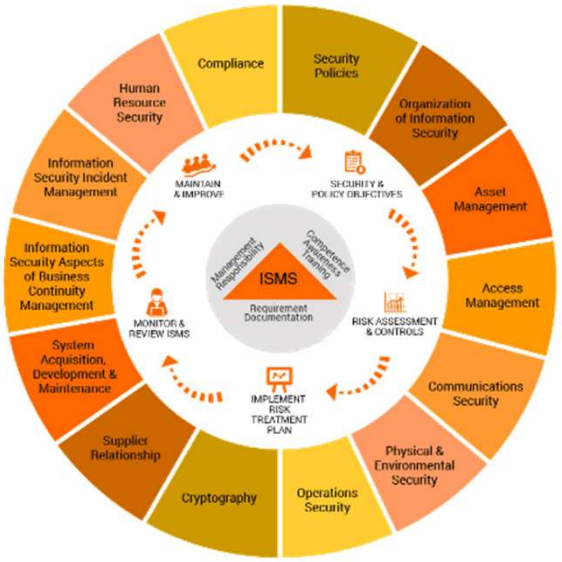




GOALS: CIA/SFU

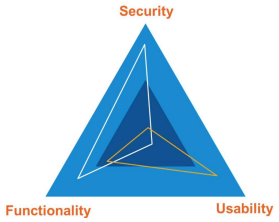
GRC: NIST, ISO 27001

PPT: People, Process, Technology




# สูตรสำเร็จ เพื่อ Cybersecurity




GOALS: Confidentiality, Integrity Availability /Security, Functionality, Usability

Governance, Risk, Compliance : NIST, ISO 27001

PPT:

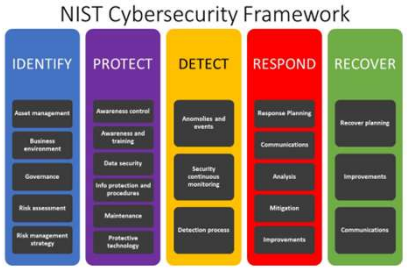
PEOPLE: SKA: Skill, Knowledge, Ability, ETA: Education, Training, Awareness,
MICE: Money, Ideology, Coercion, Ego

PROCESS: Policy, Regulation, Procedure, Cyber Drill+Practice

Technology: Identity and Access Management, Fire Wall,

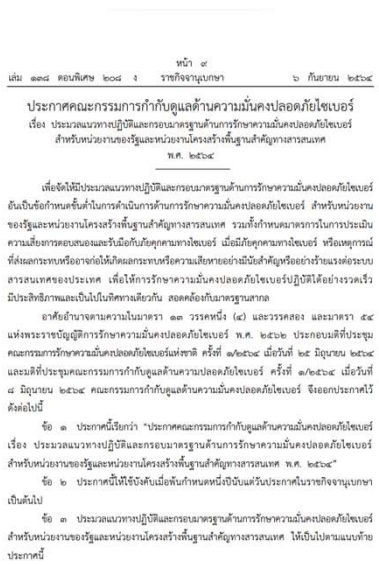
SIEM: Security information and event management, SOAR: Security Orchestration, Automation and Response, EDR: Endpoint Detection and Response , Intrusion Detection System, Intrusion Prevention System, etc

NCSA สกมช



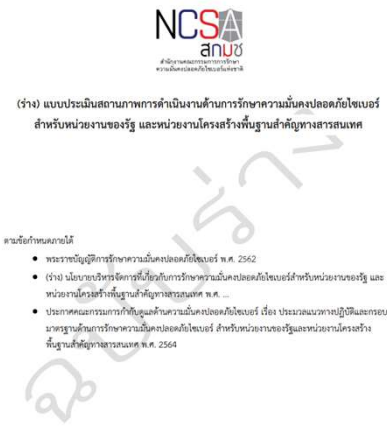

# จะเริ่มต้นได้อย่างไร?


**นโยบายและแผนปฏิบัติการฯ ด้านไซเบอร์ (พ.ศ. 2565 – 2570)**



ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔

**ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ด้านไซเบอร์ พ.ศ. 2564**



(ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

**(ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านไซเบอร์ หน่วยงานของรัฐ/CII**

# นโยบายและแผนปฏิบัติการว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)


https://drive.ncsa.or.th/s/JaqfCK9J8GtP9pH

# หน่วยงาน CII vs หน่วยงานของรัฐ ตาม พ.ร.บ.ไซเบอร์ 62

| มาตรา | หน่วยงาน CII | หน่วยงานของรัฐ* |
|---|---|---|
| 43 ดำเนินการตามนโยบายและแผนปฏิบัติการฯ | / | / |
| 44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ | / | / |
| 45 มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน | / | / |
| 46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการไปยังสำนักงาน | / | / |
| 52 แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ | / | |
| 53 รับการตรวจสอบมาตรฐานขั้นต่ำจากหน่วยงานควบคุมหรือกำกับดูแล | / | |
| 54 จัดให้มีการประเมินความเสี่ยงฯ รวมทั้งต้องจัดให้มีการตรวจสอบฯ | / | |
| 56 มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ | / | |
| 57 รายงานเหตุภัยคุกคามทางไซเบอร์ และปฏิบัติตามส่วนที่ 4 | / | |
| 58 ตรวจสอบ ประเมิน ป้องกัน รับมือ ลดความเสี่ยง ตามประมวลฯ และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว | / | / |

*หมายถึง หน่วยงานของรัฐที่มิได้เป็นหน่วยงาน CII

# นโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

## ❖ รายละเอียดโดยสรุป

**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 9 (2)** กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกันโดยใช้หลักการตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลก รวมถึงประเทศไทย ซึ่งคือ หลักการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม **ประกอบด้วย 3 หลักการ** ดังนี้


### 1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

- จัดโครงสร้างองค์กรให้มีการถ่วงดุล
- ให้มีผู้รับผิดชอบงานบริหารความมั่นคงปลอดภัยไซเบอร์
- หน่วยงานของรัฐ/หน่วยงาน CII ต้องจัดให้มี**ผู้บริหารระดับสูง**ที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

### 2. การบริหารความเสี่ยง (Risk Management)

- จัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร
- ต้องเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง
- ต้องติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอ

### 3. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

- กำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- ทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญ

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**

| | |
|---|---|
| 1 | การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) |
| 1.1 | **มีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กร พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)** |
| 1.2 | **หน่วยงานของรัฐ มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน** |
| | 1.2.1 โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์ |
| | 1.2.2 ควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ |
| 1.3 | **หน่วยงาน CII มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน** |
| | 1.3.1 ควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล |

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**

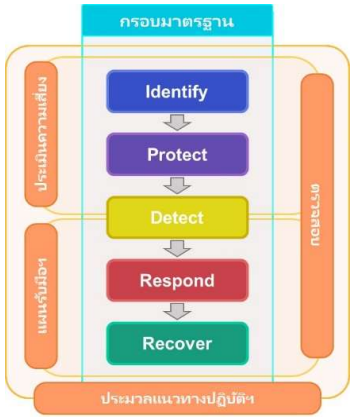
| 2 | การบริหารความเสี่ยง (Risk Management) |
|---|---|
| **2.1** | **มีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร กรอบจะรวมถึง** |
| | 2.1.1 เกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) |
| | 2.1.2 วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ |
| | 2.1.3 การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ |
| **2.2** | **มีการเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII** |
| **2.3** | **มีการติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้** |

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**

| 3 | นโยบาย และแนวปฏิบัติ (Policies and Guidelines) |
|---|---|
| **3.1** | **มีการกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII จากภัยคุกคามทางไซเบอร์** |
| | 3.1.1 นโยบาย มาตรฐาน และแนวปฏิบัติมีความสอดคล้องกับหลักประมวลแนวทางปฏิบัติที่คณะกรรมการกำหนด ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ |
| | 3.1.2 นโยบาย มาตรฐาน และแนวปฏิบัติมีการเผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII |
| **3.2** | **มีการทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงานหน่วยงานของรัฐ และหน่วยงาน CII และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละ 1 ครั้ง** |

# ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564




https://drive.ncsa.or.th/s/WB4Y5TzZJ6XEiRJ

# ประมวลแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 44 ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้
(1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
(2) แผนการรับมือภัยคุกคามทางไซเบอร์

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2

แผนการรับมือภัยคุกคามทางไซเบอร์

3

# ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| 1 | แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ |
|---|---|
| **1.1** | **มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้** |
| | 1.1.1 กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) |
| | 1.1.2 บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงาน CII เป็นเจ้าของและใช้บริการ |
| | 1.1.3 การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่ กมช. ประกาศกำหนด |
| **1.2** | **หน่วยงาน CII มีการจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด 30 (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแล** |

# ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

| 1 | แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (ต่อ) |
|---|---|
| 1.3 | **ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ระบุการไม่ปฏิบัติตามข้อ 17.1 เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงาน CII ส่งแผนการดำเนินการแก้ไขไปยัง สกมช. ภายในกำหนด 30 (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้** |
| | 1.3.1 ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงาน CII จะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม |
| | 1.3.2 กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ 17.3 (ก) |
| 1.4 | **ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงาน CII ดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยัง สกมช. ภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย** |
| 1.5 | **เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงาน CII จะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.** |

# ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| 2 | **การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** มีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้ |
| **2.1** | **การประเมินความเสี่ยง (Risk Assessment)** |
| | 2.1.1 มีการระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ |
| | 2.1.2 มีความเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม |
| | 2.1.3 มีการประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite) |
| **2.2** | **การจัดการความเสี่ยง (Risk treatment)** |
| | มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ |
| | มีการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน |

# ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| 2 | **การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)** มีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้ |
| **2.3** | **การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)** |
| | 2.3.1 มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ |
| **2.4** | **การรายงานความเสี่ยง (Risk reporting)** |
| | 2.4.1 มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ |
| | 2.4.2 มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ |

# ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนการรับมือภัยคุกคามทางไซเบอร์

| 3 | แผนการรับมือภัยคุกคามทางไซเบอร์ |
|---|---|
| 3.1 | มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) |
| 3.2 | มีการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมดอย่างมีประสิทธิผล |
| 3.3 | มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ |
| 3.4 | มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้
(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนด**กรอบมาตรฐาน**ตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์


**NIST Cybersecurity Framework**

Source: "NIST Framework for improving critical infrastructure cybersecurity", www.nist.gov/

| Functions | Cybersecurity Framework (CSF) Core Functions: |
|---|---|
| IDENTIFY | **Identify**—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. |
| PROTECT | **Protect**—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. |
| DETECT | **Detect**—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. |
| RESPOND | **Respond**—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. |
| RECOVER | **Recover**—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| 1 | การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) |
| **1.1** | **การจัดการทรัพย์สิน (Asset Management)** |
| | 1.1.1 มีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน |
| | 1.1.2 มีการระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) |
| | 1.1.3 มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย |
| | 1.1.4 มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ตามรายการที่ระบุไว้ในทะเบียนทรัพย์ในข้อ 21.1.1 อย่างน้อยปีละ 1 ครั้ง |
| **1.2** | **การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)** |
| | 1.2.1 มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด |
| | 1.2.2 มีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| 1 | **การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) (ต่อ)** |
| 1.3 | **การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)** |
| | 1.3.1 มีการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน โดยครอบคลุมบริการที่สำคัญซึ่งเป็นระบบเทคโนโลยีสารสนเทศ (Information Technology system) และระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS) |
| | 1.3.2 ขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญครอบคลุมการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม |
| | 1.3.3 มีการประเมินช่องโหว่ของบริการที่สำคัญก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ |
| | 1.3.4 ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย |
| | 1.3.5 มีการตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) ได้รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ |
| | 1.3.6 ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ตามความจำเป็น |
| | 1.3.7 มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระ |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



| | |
|---|---|
| 1 | การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) (ต่อ) |
| 1.3 | **การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) (ต่อ)** |
| | 1.3.9 มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ) |
| | 1.3.10 มีการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบให้ กกม. หรือ สกมช. ทราบภายใน 30 วันนับจากที่ได้รับการร้องขอ |
| 1.4 | **การจัดการผู้ให้บริการภายนอก (Third-Party Management)** |
| | 1.4.1 ผู้ให้บริการภายนอกต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ |
| | 1.4.2 มีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก |
| | 1.4.3 ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| **2** | **มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)** |
| **2.1** | **การควบคุมการเข้าถึง (Access Control)** |
| | 2.1.1 มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น |
| | 2.1.2 มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ |
| | 2.1.3 มีการเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ |
| | 2.1.4 มีการตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยหน่วยงาน และดำเนินการในสถานที่ หากเป็นไปได้ |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| 2 | มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) (ต่อ) |
|---|---|
| 2.2 | **การทำให้ระบบมีความแข็งแกร่ง (System Hardening)** |
| | 2.2.1 มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) |
| | 2.2.2 มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยตามข้อ 22.2.2 (ก) – 22.2.2 (ซ) |
| | 2.2.3 มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ |
| | 2.2.4 มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง |
| | 2.2.5 มีกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



| 2 | มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) (ต่อ) |
|---|---|
| 2.3 | **การเชื่อมต่อระยะไกล (Remote Connection)** |
| | 2.3.1 มีการตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ |
| | 2.3.2 มีการปฏิบัติตามแนวทางปฏิบัติในข้อ 22.3.2 (ก) – (จ) |
| 2.4 | **สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)** |
| | 2.4.1 มีการควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา กับบริการที่สำคัญ |
| | 2.4.2 มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้ |
| | 2.4.3 มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้ |
| 2.5 | **การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)** |
| | 2.5.1 แผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ |
| | 2.5.2 มีการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



| | |
|---|---|
| 2 | มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) (ต่อ) |
| 2.6 | การแบ่งปันข้อมูล (Information Sharing) |
| | 2.6.1 กำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว |

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| **3** | **มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)** |
| **3.1** | **การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)** |
| | 3.1.1 มีการสร้างกลไกและกระบวนเพื่อ ตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ |
| | 3.1.2 มีการทบทวนกลไกและกระบวนการภายในข้อ 23.1.1 อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง |

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| **4** | **มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)** |
| **4.1** | **แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)** |
| | 4.1.1 มีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง |
| **4.2** | **แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)** |
| | 4.2.1 มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ |
| | 4.2.2 มีแผนการสื่อสารในภาวะวิกฤต ซึ่งกำหนดรายละเอียดตามข้อ 24.2.2 (ก) – (จ) |
| | 4.2.3 มีการตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ |
| **4.3** | **มีการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง** |

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

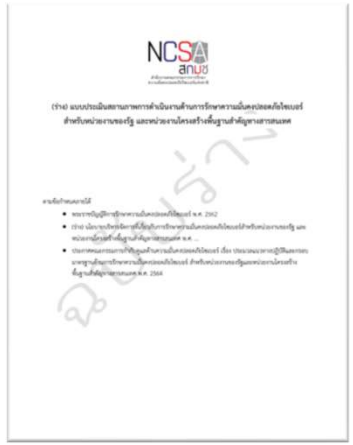
| 4 | มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) (ต่อ) |
|---|---|
| 4.4 | **การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)** |
| | 4.4.1 มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน |
| | 4.4.2 มีการตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ |
| | 4.4.3 มีการปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ |

# แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์**

| | |
|---|---|
| 5 | การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) |
| **5.1** | **การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)** |
| | 5.1.1 มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) |
| | 5.1.2 มีการฝึกซ้อม BCP อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง |

# (ร่าง) แบบประเมินสถานภาพการดำเนินงาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ/หน่วยงาน CII



https://drive.ncsa.or.th/s/Yz4pEB9g3dqfqXK

# (ร่าง) แบบประเมินสถานภาพการดำเนินงานฯ

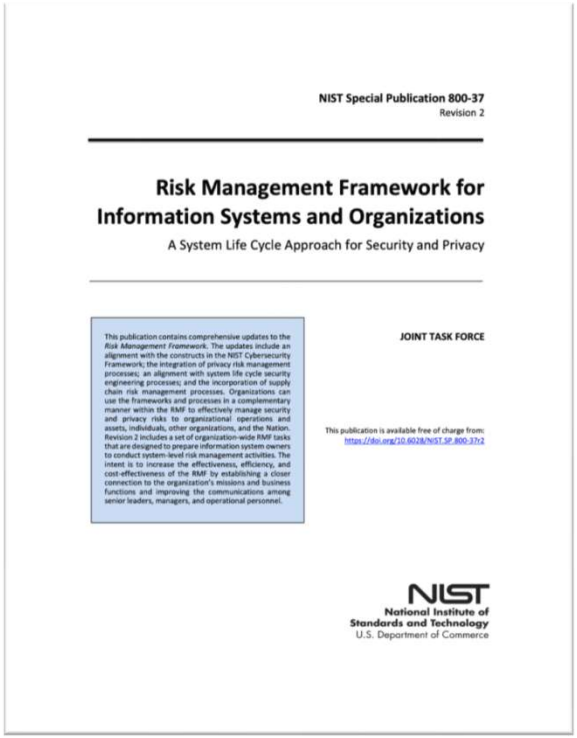
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (8 ข้อ)

ประมวลแนวทางปฏิบัติ (3 ข้อ) และกรอบมาตรฐาน (15 ข้อ)

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ /CII (3 ข้อ)

# มีกระบวนการอย่างไร?

## การ implement NIST CSF โดยใช้ NIST SP 800-37 (RMF)



NIST Special Publication 800-37
Revision 2

**Risk Management Framework for Information Systems and Organizations**

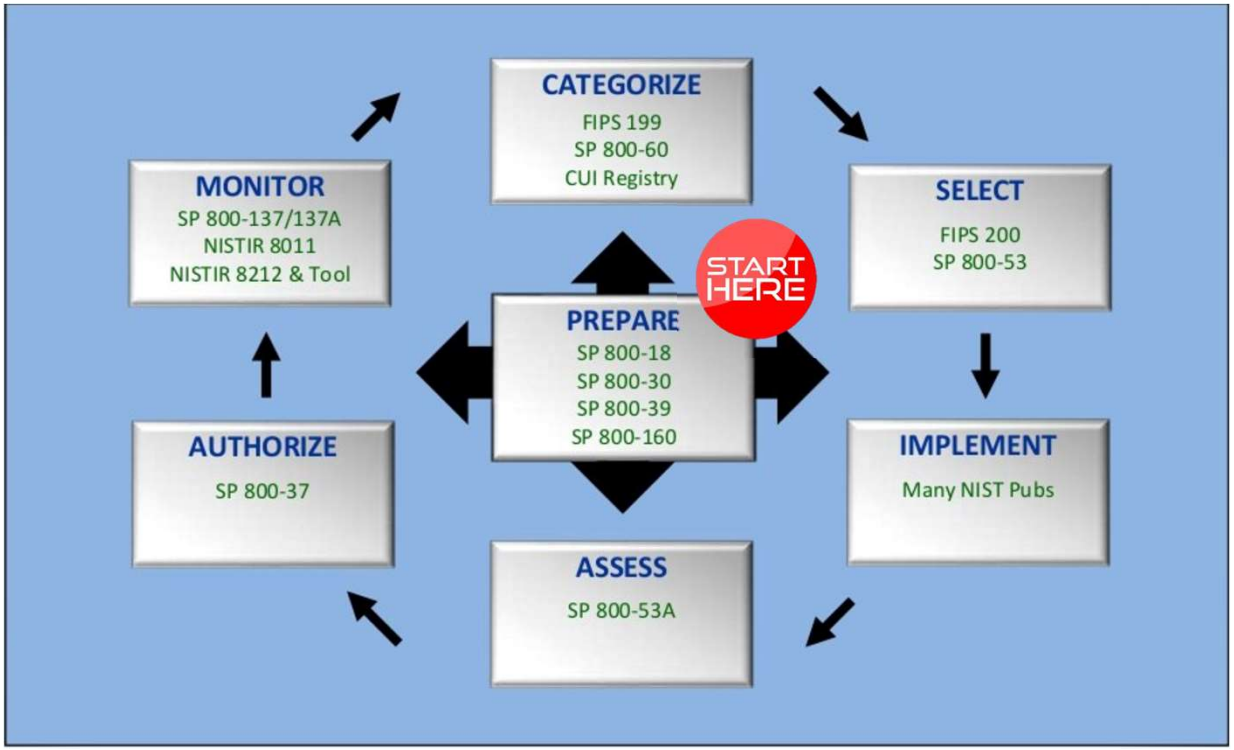
A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

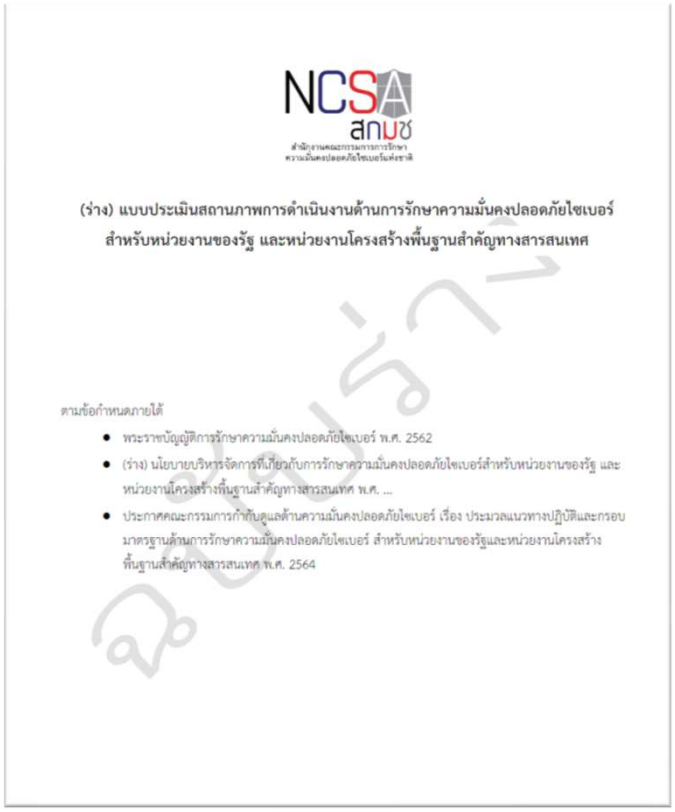
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce




Ref : https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

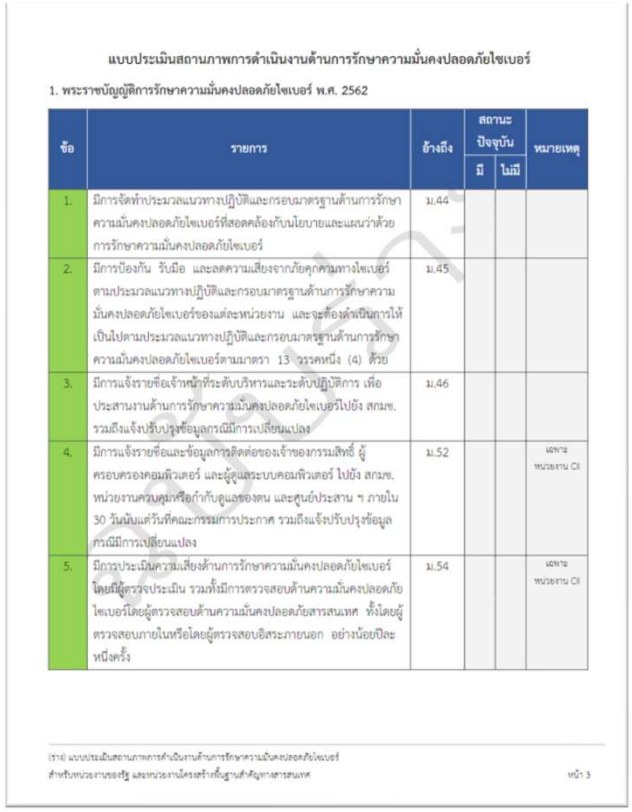
# (ร่าง) แบบประเมินสถานภาพการดำเนินงานฯ



(ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ตามข้อกำหนดภายใต้

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ...
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

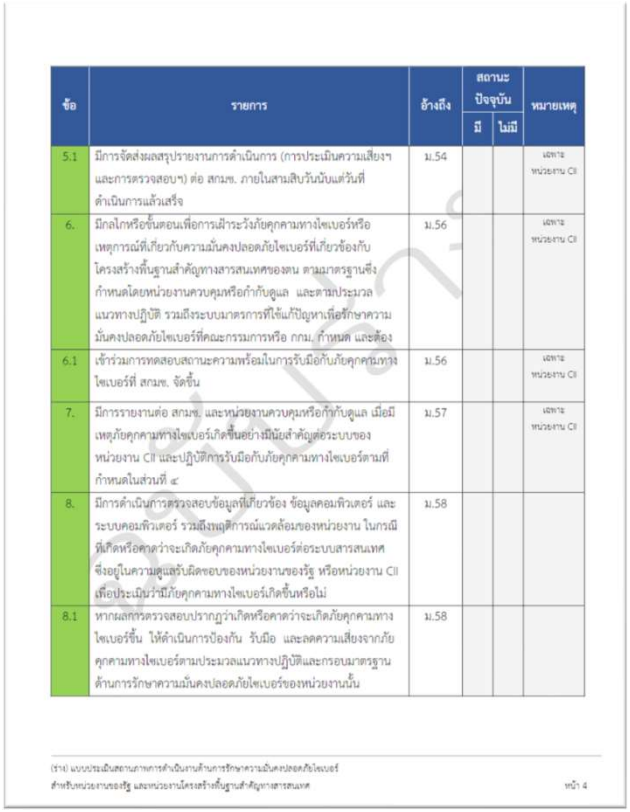


แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

| ข้อ | รายการ | อ้างถึง | สถานะปัจจุบัน | | หมายเหตุ |
|---|---|---|---|---|---|
| | | | มี | ไม่มี | |
| 1. | มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ | ม.44 | | | |
| 2. | มีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 13 วรรคหนึ่ง (4) ด้วย | ม.45 | | | |
| 3. | มีการแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช. รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง | ม.46 | | | |
| 4. | มีการแจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ ไปยัง สกมช. หน่วยงานควบคุมหรือกำกับดูแลของตน และศูนย์ประสาน ฯ ภายใน 30 วันนับแต่วันที่คณะกรรมการประกาศ รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง | ม.52 | | | เฉพาะหน่วยงาน CII |
| 5. | มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง | ม.54 | | | เฉพาะหน่วยงาน CII |





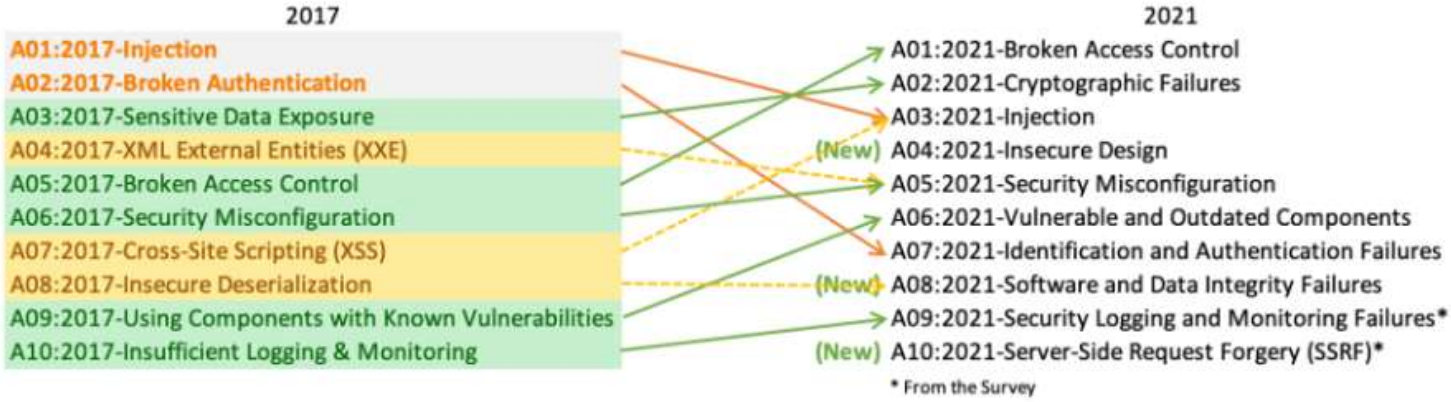
| ข้อ | รายการ | อ้างถึง | สถานะปัจจุบัน | | หมายเหตุ |
|---|---|---|---|---|---|
| | | | มี | ไม่มี | |
| 5.1 | มีการจัดส่งผลสรุปรายงานการดำเนินการ (การประเมินความเสี่ยงฯ และการตรวจสอบฯ) ต่อ สกมช. ภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ | ม.54 | | | เฉพาะหน่วยงาน CII |
| 6. | มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้อง | ม.56 | | | เฉพาะหน่วยงาน CII |
| 6.1 | เข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่ สกมช. จัดขึ้น | ม.56 | | | เฉพาะหน่วยงาน CII |
| 7. | มีการรายงานต่อ สกมช. และหน่วยงานควบคุมหรือกำกับดูแล เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงาน CII และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ | ม.57 | | | เฉพาะหน่วยงาน CII |
| 8. | มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ รวมถึงเหตุการณ์แวดล้อมของหน่วยงาน ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐ หรือหน่วยงาน CII เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ | ม.58 | | | |
| 8.1 | หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น | ม.58 | | | |

# คำแนะนำสำหรับการ Hardening ระบบ Website

อ้างอิง https://blog.sucuri.net/2022/11/top-12-website-hardening-tips.html

# OWASP Top Ten

OWASP หรือ Open Web Application Security Project คือ มาตราฐานความปลอดภัยของเว็บแอปพลิเคชัน ซึ่งได้ทำการจัดอันดับช่องโหว่ที่มีความรุนแรง และพบเจอได้บ่อยในเว็บแอปพลิเคชัน 10 อันดับแรก และได้รับการตอบรับเป็นอย่างดีจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลก โดยยึดถือเป็นมาตรฐานการตรวจสอบช่องโหว่เว็บแอปพลิเคชัน ที่อธิบายรายละเอียดของช่องโหว่ที่พบได้บ่อยและมีความรุนแรง 10 อันดับแรก



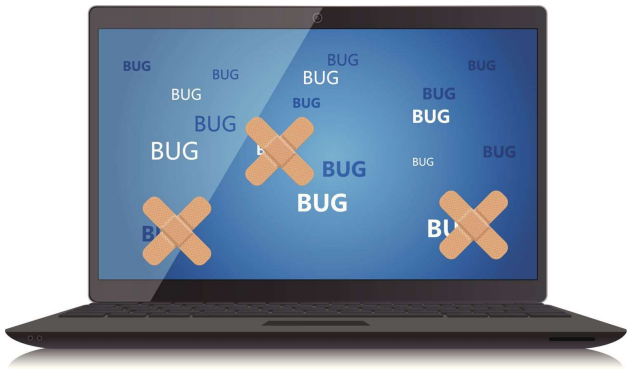

อ้างอิง https://owasp.org/www-project-top-ten/

# 1 – Keep your website patched and updated

ซอฟต์แวร์ทุกอย่างที่ทำงานบนเว็บไซต์ ต้องได้รับการปรับปรุงให้ทันสมัยด้วยแพตช์ล่าสุดและการอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ ดังนั้นจึงเป็นเรื่องสำคัญที่จะต้องอัปเดต เช่น

- ระบบ CMS พร้อมกับส่วนประกอบภายใน เช่น ปลั๊กอิน ธีม และส่วนขยายต่างๆ
- ระบบ Webserver เช่น Apache หรือ PHP updates
- ระบบปฏิบัติการ

☑ การทำให้ทุกอย่างเป็นปัจจุบันด้วยการอัปเดตล่าสุด จะลดความเสี่ยงที่ผู้โจมตีพุ่งเป้าไปยังเว็บไซต์จากช่องโหว่ที่รู้จัก



# 2 – Reduce your attack surface

อนุญาตให้เข้าถึง public access port ของแอปพลิเคชันเท่านั้น เช่น

- เปิด port ที่จำเป็นต้องใช้เท่านั้น เช่น HTTP – Port 80, HTTPS – 443, FTPS / SSH – 22.
- ควรปรับการตั้งค่า Disable Server Banners

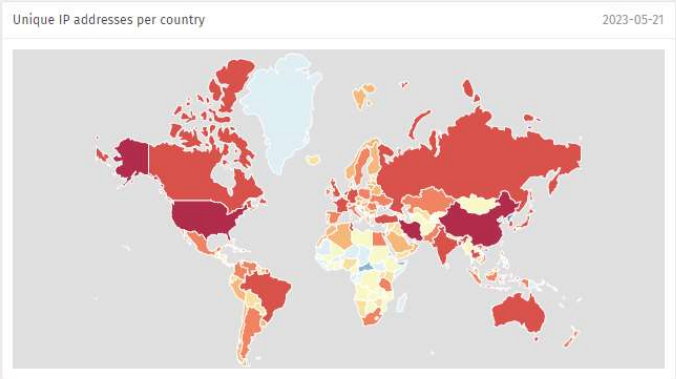
```
root@kali:~# curl -s -I 192.168.0.11
HTTP/1.1 200 OK
Date: Fri, 03 Jul 2020 19:11:08 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Sun, 21 Jun 2020 19:07:07 GMT
ETag: "2aa6-5a89cd520737c"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html
```

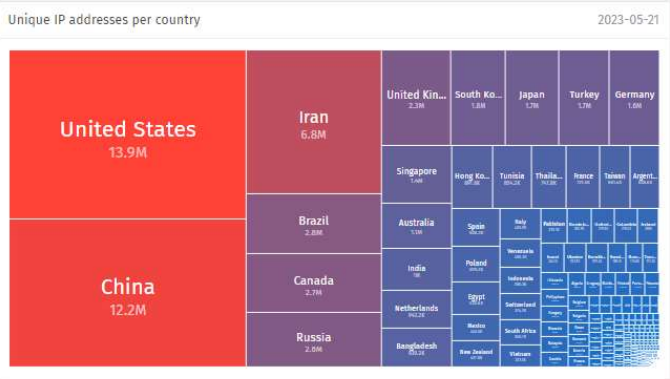
```
# Nmap 7.80 scan initiated Mon Feb  3 10:51:59 2020 as: nmap --max-
Nmap scan report for [redacted]
Host is up (0.024s latency).
Not shown: 986 filtered ports
PORT      STATE  SERVICE
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
2000/tcp  open   cisco-sccp
5060/tcp  open   sip
5061/tcp  open   sip-tls
8008/tcp  open   http
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
49155/tcp open   unknown
50001/tcp open   unknown
50002/tcp open   iiimsf
50003/tcp open   unknown
# Nmap done at Mon Feb  3 20:52:04 2020 -- 1 IP address (1 host up)
```

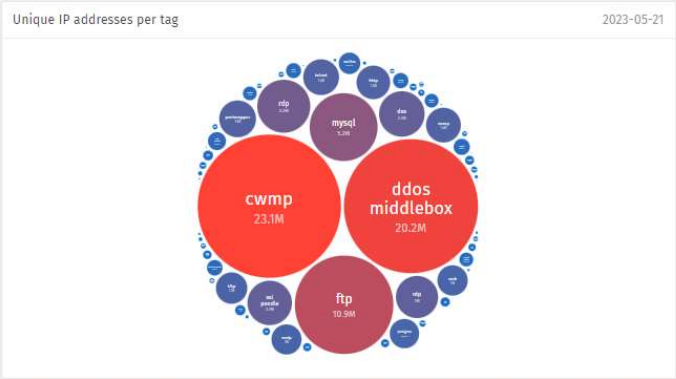
# 2 – Reduce your attack surface (ต่อ)

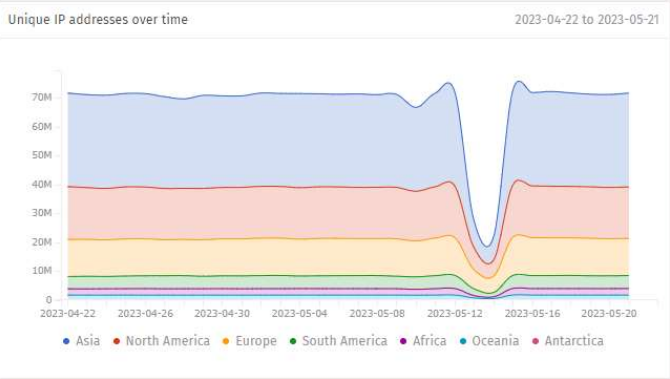
Shadowserver scans the entire IPv4 Internet for over 100 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols. These are “hello” type port scans that do not exploit any vulnerability. They enable identification of misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or simply just population enumeration. Population enumeration results can be found under the “population” source type.

https://dashboard.shadowserver.org/



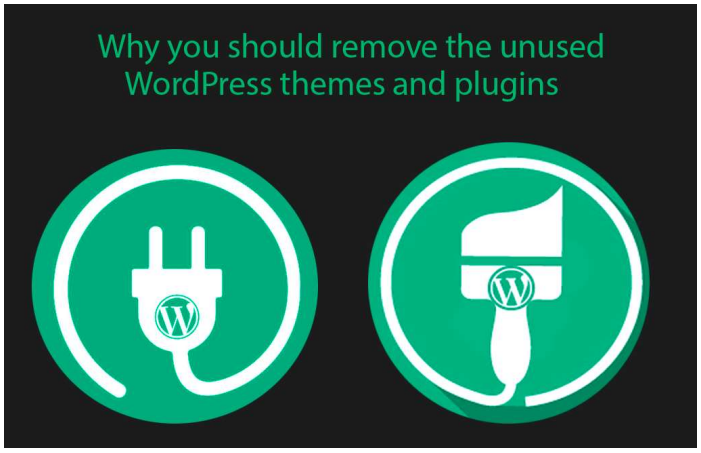



# 3 – Remove unnecessary plugins and themes

ฟีเจอร์และฟังก์ชันการทำงานที่ปรับปรุงการมีส่วนร่วมและประสบการณ์เว็บไซต์ แต่ยิ่งมีซอฟต์แวร์ (third-party components) มากเท่าใดความเสี่ยงที่จะถูกโจมตีก็จะยิ่งมากขึ้นเท่านั้น plugins and themes เพิ่มเติมในเว็บไซต์เป็นช่องทางที่เป็นไปได้สำหรับการโจมตี



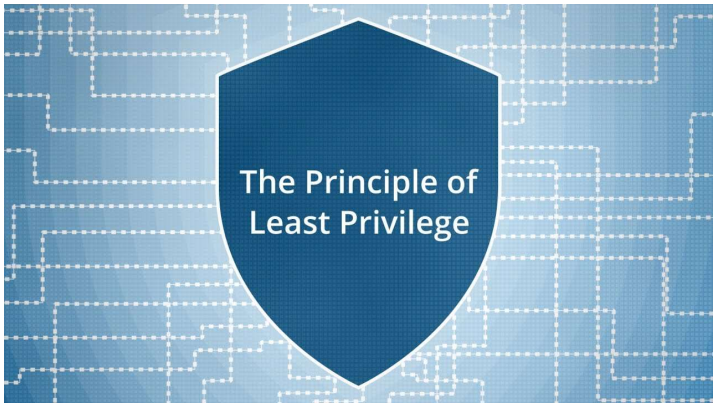
# 4 – Practice the principle of least privilege

จำกัดสิทธิ์ที่สมาชิกในทีมดูแลเว็บไซต์สามารถทำได้ และตรวจสอบให้แน่ใจว่าตามหน้าที่ไม่มีสิทธิพิเศษมากเกินความจำเป็น สิ่งนี้สามารถทำได้โดยปฏิบัติตามหลักการของ least privilege

ตัวอย่างเช่น หากมี editor ที่ดูแลเนื้อหาเว็บไซต์ ก็ไม่จำเป็นต้องให้มีสิทธิ์ของผู้ดูแลระบบ

There are 5 roles built into WordPress,
plus 1 that's only seen in multisite installations,
for a total of 6 user roles. The roles are:

- Subscriber
- Contributor
- Author
- Editor
- Administrator
- Super Admin (multi-site only)



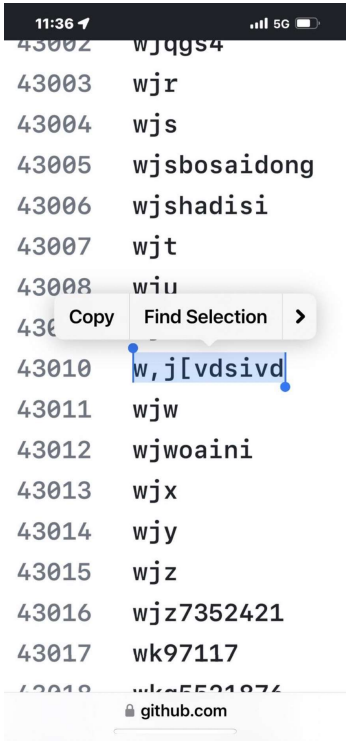
# 5 – Restrict access to your admin panel

การเข้าสู่ระบบแผงของผู้ดูแลระบบ CMS เช่น WordPress ที่สามารถเข้าถึงได้โดยสาธารณะ สิ่งนี้ทำให้เสี่ยงต่อการถูกโจมตี

การเพิ่มความปลอดภัยของแผงผู้ดูแลระบบ

- ปรับเปลี่ยน Link Login สำหรับ Admin /wp-login.php
- จำกัดความพยายามในการ Login
- ใช้ CAPTCHA

# 6 – Use strong, unique passwords




รหัสผ่าน w,j[vdsivd
ปลอดภัยหรือไม่?

ข้อมูลจาก https://github.com/buyanov/passwords/blob/master/dict.txt

# 6 – Use strong, unique passwords (ต่อ)

ควรมีอักขระอย่างน้อย 10 ตัว แต่มากกว่า 14 ตัวจะยิ่งดีขึ้น ชุดอักษรตัวพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และสัญลักษณ์ ไม่ใช่หนึ่งในพจนานุกรมหรือชื่อของบุคคล อักขระ ผลิตภัณฑ์ หรือองค์กร ไม่ควรใช้ข้อมูลส่วนตัวที่หาได้ง่าย ชื่อ วันเดือนปีเกิด เลขบัตรประชาชน มาตั้งรหัสผ่าน

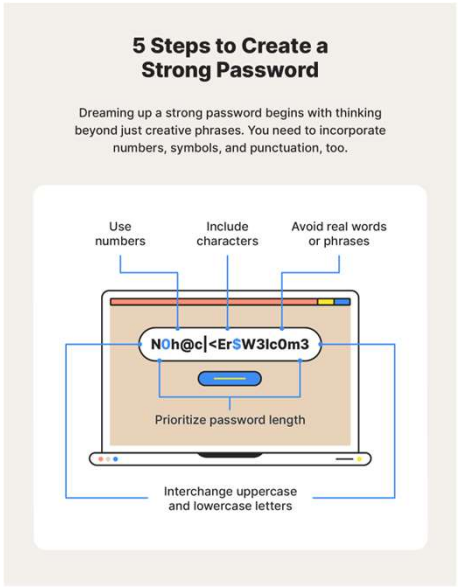
**Password Strength Chart**

SANDSTORM IT

This is based on the average brute forcing (botnet) power in 2019.

| | | |
|---|---|---|
| 123456<br>Top 10,000 password | 0.20 milliseconds | Unsafe |
| qwerty123456<br>Longer "common" password | 13 hours | Unsafe |
| ITFunSom3times<br>Longer password with numbers | 48 thousand years | Risky |
| ITi$fun$0m3times!<br>Longer password with numbers and special characters | 13 trillion years | Good |
| imusingalongpasswordtoday<br>Even Longer password | 913 trillion years | Better |
| imu$inga1ongpa$$word+oday!<br>Even Longer password with numbers and special characters | 2 octillion years | Best |

Please Note: These passwords are for demonstration purposes ONLY and are not to be used.



# 7 – Use multi-factor authentication

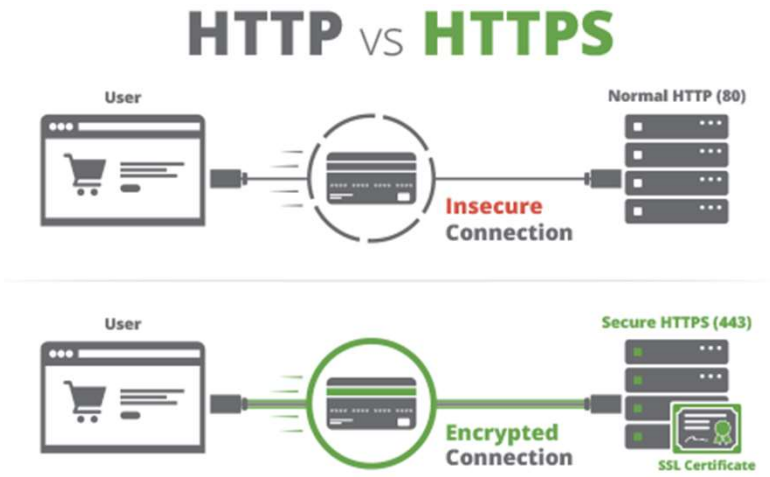
การรับรองความถูกต้องด้วยหลายปัจจัยเป็นวิธีการรับรองความถูกต้องหลายวิธีจากข้อมูลประจำตัวประเภทต่างๆ เพื่อยืนยันตัวตนของผู้ใช้ โดยพื้นฐานแล้วเป็นการรวมรูปแบบการรับรองความถูกต้องที่เป็นอิสระจากกันตั้งแต่สองรูปแบบขึ้นไป

ตัวอย่าง

- Something you know (a password)
- Something you have (a security token, OTP)
- Something you are (biometrics)

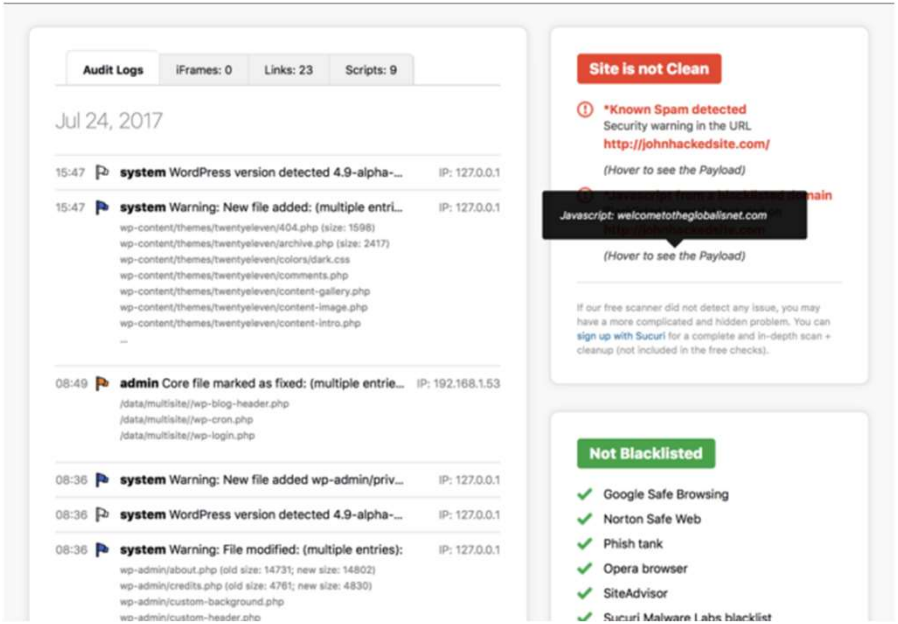
# 8 – Access over HTTPS

เว็บไซต์ควรเข้าถึงผ่าน HTTPS —ข้อมูลทั้งหมดได้รับการเข้ารหัสอย่างปลอดภัยระหว่างการส่งจากจุด A ไปยังจุด B SSL Certificate คือ ใบรับรองอิเล็กทรอนิกส์ เป็นไฟล์ข้อมูลขนาดเล็ก ที่ได้มีการผูกไว้กับ Private Key ของเครื่องเซิร์ฟเวอร์ เพื่อยืนยันตัวตนและความถูกต้องในการส่งข้อมูลระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน มีการเข้ารหัสและถอดรหัสผ่านเทคโนโลยี SSL/TLS หากข้อมูลถูกดักจับไปได้ ข้อมูลก็ยังมีความปลอดภัย เพราะแฮกเกอร์ จะไม่สามารถถอดรหัสข้อมูลได้

# 9 – Monitor your website and keep up with its log activity

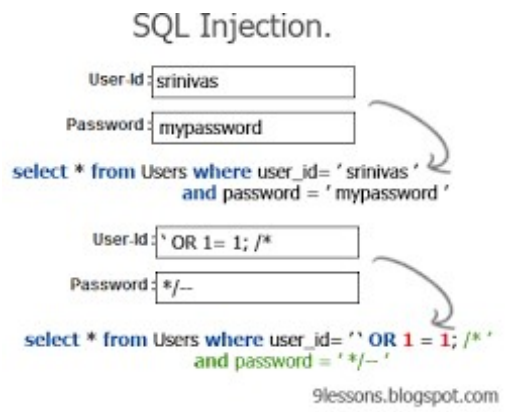
Log มีความสำคัญสำหรับการตรวจสอบเว็บไซต์ นอกจากนี้ยังมีประโยชน์มากเมื่อต้องการแก้ไขปัญหาทางเทคนิคหรือตรวจสอบความรับผิดชอบของผู้ใช้ ควรมีการเก็บ Log กิจกรรมต่างๆ ของเว็บไซต์เพื่อสามารถนำมาตรวจสอบหรือวิเคราะห์กิจกรรมต่างๆ เมื่อเกิดปัญหาขึ้น

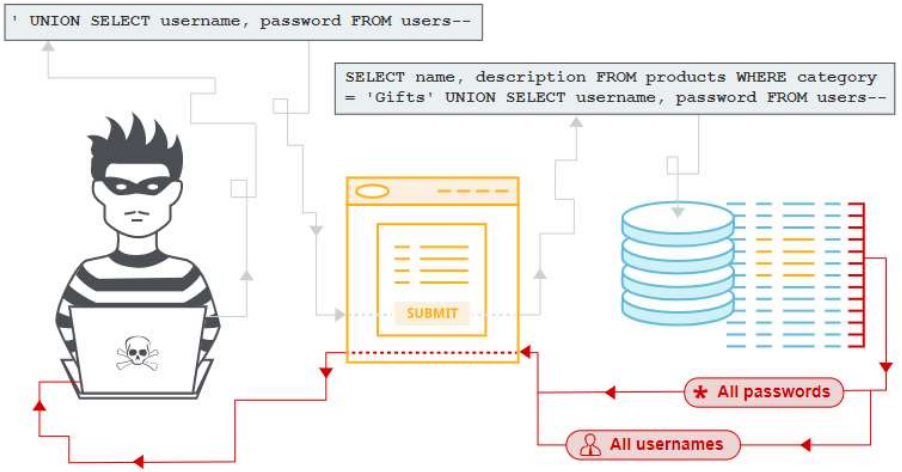


# 10 – Use input sanitization techniques

Input sanitization จะเป็นการกรองข้อมูล Input ที่เข้ามาสู่เว็บไซต์ นอกจากนี้ยังป้องกันการโจมตีจาก SQL injection attacks หรือ Cross-site-scripting (XSS) ควรมีมาตรการป้องกัน Input เช่น

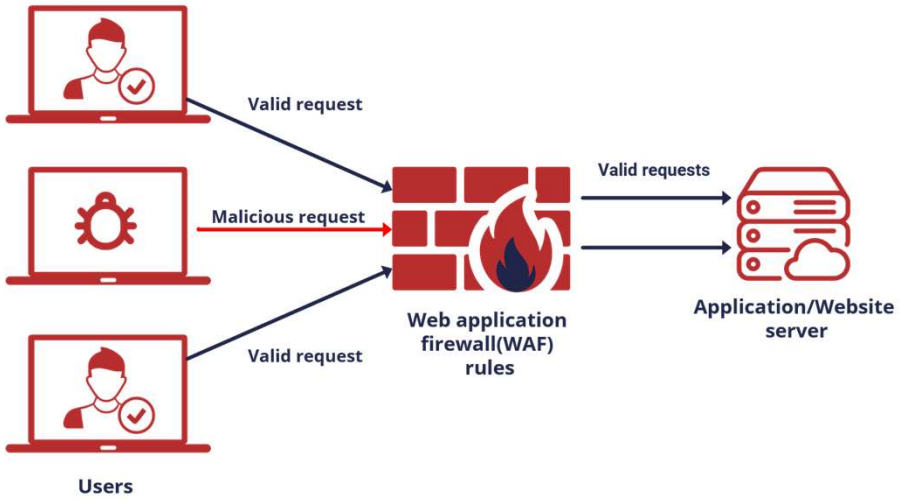
- การรับ Input ที่เป็น อักขระพิเศษ
- จำกัดความยาวตัวอักษรของ Input
- การรับชนิดของ Input เช่น เป็นตัวอักษร หรือ ตัวเลข เป็นต้น



# 11 – Use a web application firewall

Web Application Firewall (WAF) เป็นเครื่องมือที่ใช้ป้องกัน Web application จากการโจมตีผ่านทาง Application Layer ช่วยปกป้องเว็บแอปพลิเคชันโดยการกรองและตรวจสอบปริมาณข้อมูล HTTP ระหว่างเว็บแอปพลิเคชันและอินเทอร์เน็ตโดยทั่วไปจะปกป้องเว็บแอปพลิเคชันจากการโจมตี เช่น DDoS Protection , Cross-site-scripting (XSS) , และ SQL-injection



# Q / A

ช่องทางติดต่อสำหรับคำแนะนำ
อีเมล thaicert@ncsa.or.th


สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

Youtube NCSA Thailand
Website https://www.ncsa.or.th/
Facebook NCSA Thailand

"Protection is better than cure"