Saraburi Ransomware Attack

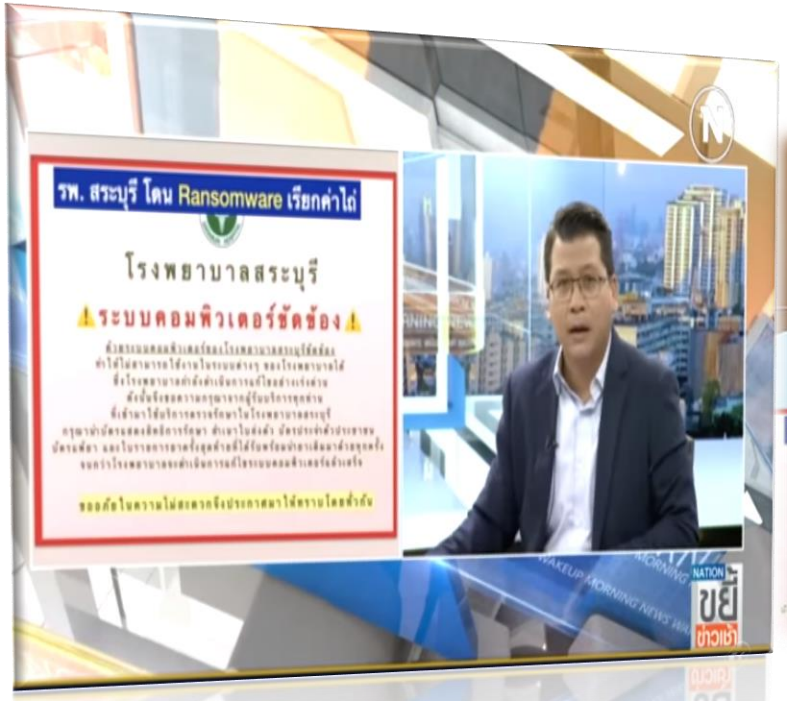
Leaning point

นายแพทย์อนันต์ กมลเนตร

ผู้อำนวยการโรงพยาบาลสระบุรี

19 มกราคม 2566

สถานการณ์การถูกโจมตี
ระบบฐานข้อมูลโรงพยาบาลสระบุรี



สรุปความเสียหาย

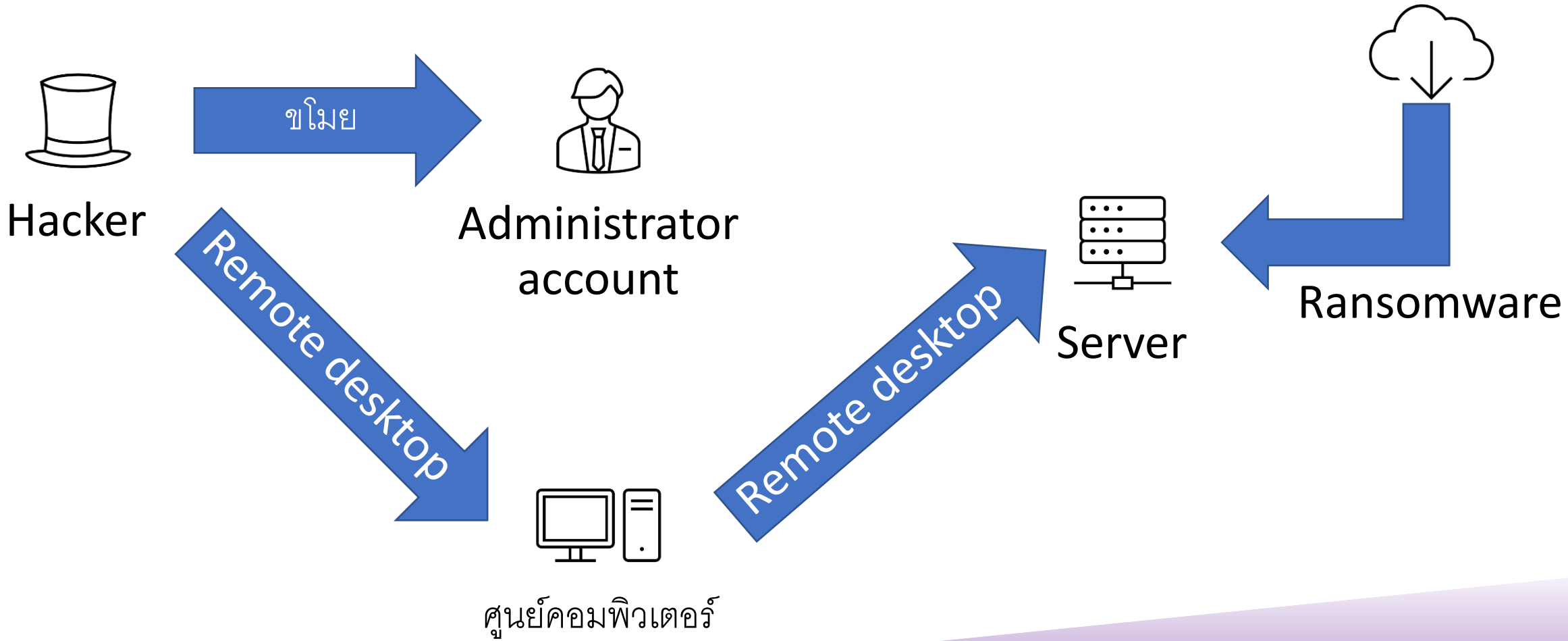
ฐานข้อมูลผู้ป่วย ไม่สามารถใช้งานได้

ภาพสแกนเวชระเบียนผู้ป่วยเสียหายทั้งหมด

เครื่องแม่ข่าย ให้บริการไม่ได้

ระบบเครือข่าย/ระบบโทรศัพท์ไม่สามารถใช้งานได้

ผลการวิเคราะห์เบื้องต้นจาก ThaiCERT



ปัจจัยสำคัญที่พบจากการทำ RCA

Policy

- มีนโยบายเรื่องการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศและความปลอดภัย
- ไม่ปฏิบัติตามนโยบาย ไม่มีบทลงโทษ

Hardware Software

- Software ไม่มี License; ขาดการ Update
- ขาด Software และ Hardware ที่จำเป็นต่อการป้องกัน

ปัจจัยสำคัญที่พบจากการทำ RCA

System architecture

- Easy to use – Less Security

Authority

- ให้สิทธิ์มากเกินความจำเป็น – ได้สิทธิ์ Admin ที่เข้าระบบได้หมดทั้งที่ตนเองไม่มีภาระหน้าที่ในการดูแลระบบ

ปัจจัยสำคัญที่พบจากการทำ RCA

Awareness

- ขาดความเฉลี่ยวใจ/ประมาท – Drive กลางของโรงพยาบาลติดไวรัส 1 สัปดาห์ก่อนการโจมตี; พบโปรแกรมแปลกๆที่ไม่เคยพบมาก่อน
- ดาวน์โหลดไฟล์แปลกปลอม หรือการเปิด mail ที่ไม่รู้จัก

User

- ให้ Username และ Password ให้ผู้อื่น
- ตั้งรหัสผ่านไม่รัดกุมและไม่ปลอดภัย - ไม่เปลี่ยนรหัสผ่านตามข้อกำหนดขององค์กร
- ติดตั้ง Software เอง

การปรับปรุงความปลอดภัยระบบสารสนเทศ - การจัดการ

ปรับเปลี่ยนผังเครือข่าย

- แยกวง LAN ของ PC ที่ใช้ในระบบสารสนเทศรพ. (SSB, SBHClinic ฯลฯ) ออกจาก PC ที่ใช้ทำงานอื่น ๆ
- จัดแยก zone ของ server และการเข้าใช้งานตามความจำเป็น

จัดระบบการสำรองข้อมูลแบบ offline โดยแยกอุปกรณ์จัดเก็บสลับวัน

ยกเลิกการแชร์ไฟล์ในเครือข่าย (DriveZ) โดยพิจารณาเปลี่ยนเป็น Google Drive แทน

การให้สิทธิตามความจำเป็น

- ปรับลดระดับ log in จากเดิมที่เป็น admin ของ Pc เป็น user ธรรมดา

การปรับปรุงความปลอดภัยระบบสารสนเทศ - การจัดการ

อนุญาตให้เข้าเว็บไซท์/ใช้งานโปรแกรมตามความจำเป็นในการทำงาน

ควบคุมการนำข้อมูลเข้า-ออกจากระบบ เช่น การจำกัดการใช้งาน flash drive/external hard disk

ThaiCert ให้คำแนะนำในการออกแบบระบบความปลอดภัยเครือข่ายใหม่

Monitor เครือข่ายของรพ.แบบ real-time

ย้าย Server ที่เป็นหัวใจสำคัญในระบบสารสนเทศรพ. ขึ้นระบบ Virtualization

- เปลี่ยนโครงสร้างระบบ Server ให้เป็น Virtualization เพื่อให้สามารถ restore การทำงานกลับมาได้รวดเร็วขึ้น

NIST Framework

	Identify	Protection	Detect	Response	Recover
ปฏิบัติแล้ว	-Risk assessment -Asset management -Risk management Strategy	-Basic Network access control -Security Training program -Next-Gen Firewall protection -Anti-Virus	-Log -Next-gen Firewall -Anti-virus	-BCP/IAP	-Offline backup
วางแผนดำเนินการ	-Full Risk assessment with Penetrating test -Revise Asset management	-Multi-factors Authentication -Per account/Per Device Network access control -Data Encryption On HIS -Apply XDR Concept	-Rental SOC, NOC -Network monitoring -XDR anti-virus anti malware	-Revise BCP/IAP	-Backup Appliance: Isolated Recovery Environment