Cybersecurity & Threat Risks: Where are we and where are we going?

6/1/2018

PROTECTION CRIMINAL DDOS PHISHING
GROUPS HACKING FIREWALL MALWARE

CYBERCRIME

COMPUTER INFECTED TROJAN VIRUS
NETWORK DIGITAL DETECTION
HACKER INTERNET INTRUDER SPYWARE SPAM

DATA CAN “SLEEP WALK”–KEEP IT SAFE

✓ UNINTENTIONAL DATA LOSS
✓ CONFIDENTIAL DATA LEAVES THE COMPANY – WITHOUT AUTHORIZED PERMISSION
✓ SYSTEMS ARE PURCHASED WITHOUT KNOWLEDGE OR SIGN-OFF BY IT [SHADOW IT]
✓ DATA STORED OUTSIDE OF IT CONTROLS IN THE CLOUD
✓ 3RD PARTY VENDOR CONCERNS
DATA CAN "SLEEP WALK"–KEEP IT SAFE

✓ PROTECTING DATA IS CRITICAL TO AN ORGANIZATION
  ◆ PRIVACY CONCERNS
  ◆ INTELLECTUAL PROPERTY
  ◆ MANY LAWS PROTECTING – NEWLY ADDED GENERAL DATA PROTECTION REGULATION (GDPR)
  ◆ GDPR PENALTIES – GREATER OF $20 MILLION (US) OR 4% OF VIOLATORS ORG GLOBAL REVENUE

WHAT IS GDPR?
  ◆ THE EUROPEAN UNION’S GENERAL DATA PROTECTION REGULATION (GDPR), IS THE BASIC FRAMEWORK FOR PROTECTION OF PERSONAL INFORMATION OF EU CITIZENS.
  ◆ THE GDPR LAYS OUT DETAILED REQUIREMENTS GOVERNING THE COLLECTION, USE, SHARING AND PROTECTION OF PERSONAL INFORMATION.
  ◆ GDPR WAS ADOPTED IN APRIL 2016 AND WENT IN FORCE ON MAY 25, 2018.

DATA CAN "SLEEP WALK"–KEEP IT SAFE

✓ GDPR – FORCES COMPANIES TO CONTROL THEIR OTHERS DATA
  ◆ LAWFUL, FAIR AND TRANSPARENT PROCESSING
  ◆ LIMITATION OF PURPOSE, DATA AND STORAGE
  ◆ DATA SUBJECT RIGHTS
  ◆ CONSENT
  ◆ PERSONAL DATA BREACHES
  ◆ DATA PROTECTION IMPACT ASSESSMENT
  ◆ DATA TRANSFERS
  ◆ DATA PROTECTION OFFICER
  ◆ AWARENESS AND TRAINING
DATA CAN "SLEEP WALK"—KEEP IT SAFE
✓ GDPR — IS IT COMING TO THE USA?
✓ MAYBE...
  ✓ FACEBOOK AND CAMBRIDGE ANALYTICA FALLOUT
  ✓ RESEARCHERS IN 2014 ASKED USERS TO TAKE A PERSONALITY SURVEY
  ✓ APP WAS ALLOWED TO COLLECT USER DATA
  ✓ 20 MILLION RAW PROFILES HARVESTED — 2.70 MILLION USERS HAD CONSENTED
  ✓ LEARNED ABOUT IT IN 2015 — DATA SHOULD HAVE BEEN DELETED — VERIFY IF IT WAS DELETED???
  ✓ WHAT WILL HAPPEN???

DATA BREACH EXAMPLES
✓ ACCIDENTALLY PUBLISHED...
  ✓ RED CROSS BLOOD SERVICE — AUSTRALIA
  ✓ OCCURRED OCT 2014
  ✓ UNSECURED DATA WAS POSTED ON A WEBSITE BY A CONTRACTOR
  ✓ LEAK INCLUDED ID INFO "PERSONAL DETAILS" OF 350,000 DONORS
  ✓ INCLUDED ANSWERS TO QUESTIONNAIRE WITH VERY PERSONAL INFO
  ✓ LARGEST DATA LEAK IN AUSTRALIA
  ✓ SECURITY PROFESSIONAL WAS CONTACTED BY SOMEONE WHO ACQUIRED THE INFORMATION. SECURITY PRO PART OF THE LEAK. SENT 1.74 GB FILE INC "AT RISK SEXUAL ACTIVITY!"

DATA BREACH EXAMPLES (CONT)
✓ PREVENTION...
✓ IMPLEMENT THE APPROPRIATE CONTRACTUAL REQUIREMENTS OR CONTROL MEASURE IN ORDER TO PROTECT PERSONAL INFORMATION THAT IS HANDLED BY A THIRD PARTY PROVIDER.
DATA BREACH EXAMPLES (CONT)

✓ HACKED...
   ▪ QUEST DIAGNOSTICS – NEW JERSEY
   ▪ OCCURRED NOV 26, 2016
   ▪ ACCESSED MYQUEST BY CARE360 INTERNET APPLICATION
   ▪ OBTAINED PHI DATA OF APPROXIMATELY 34,000 INDIVIDUALS
   ▪ THE ACCESSED DATA INCLUDED NAME, DATE OF BIRTH, LAB RESULTS, AND IN SOME INSTANCES, TELEPHONE NUMBERS.

DATA BREACH EXAMPLES (CONT)

✓ PENALTY...
   ▪ ACTIONS STILL PENDING

✓ PREVENTION...
   ▪ PATCH AND UPDATE SERVERS, REVIEW APPLICATIONS FOR POSSIBLE SECURITY ISSUES

DATA BREACH EXAMPLES (CONT)

✓ INSIDE JOB...
   ▪ FRENCH POLICE HEALTH INSURANCE
   ▪ OCCURRED JUNE 2, 2016
   ▪ PERSONAL DETAILS OF 112,00 FRENCH POLICE OFFICERS UPLOADED TO GOOGLE DRIVE
   ▪ DISGRUNTLED WORKER UPLOADED DATA
   ▪ LUCKILY THE FILES WERE PROTECTED BY A PASSWORD
DATA BREACH EXAMPLES (CONT)

✓ PREVENTION...
  • BLOCK ACCESS TO FILE SHARING SITES, MONITOR FOR DATA LEAKAGE

DATA BREACH EXAMPLES (CONT)

✓ LOST/STOLEN DEVICE AND MEDIA...
  • ADVOCATE HEALTH CARE
  • OCCURRED JULY 2013 AND NOV 2013
  • BREACH INVOLVED ELECTRONIC HEALTH INFO OF 4 MILLION PEOPLE

DATA BREACH EXAMPLES (CONT)

✓ THREE SEPARATE EVENTS...
  • FOUR UNENCRYPTED LAPTOPS WITH PERSONAL HEALTH INFORMATION WERE STOLEN FROM AN ADMINISTRATIVE OFFICE IN PARK RIDGE.
  • UNAUTHORIZED THIRD PARTY ACCESSED THE NETWORK OF AN ADVOCATE BUSINESS ASSOCIATE, POTENTIALLY COMPROMISING THE INFORMATION OF MORE THAN 2,000 PATIENTS
  • UNENCRYPTED LAPTOP WITH PERSONAL INFORMATION OF MORE THAN 2,100 INDIVIDUALS WAS STOLEN FROM THE VEHICLE OF AN ADVOCATE MEDICAL GROUP EMPLOYEE
DATA BREACH EXAMPLES (CONT)

✓ PENALTY...
  ✷ PAID $6.55 MILLION TO HHS

✓ PREVENTION...
  ✷ POLICIES AND PROCEDURES AND FACILITY ACCESS CONTROLS TO LIMIT PHYSICAL ACCESS TO THE ELECTRONIC INFORMATION SYSTEMS HOUSED WITHIN A LARGE DATA SUPPORT CENTER, ACCORDING TO OCR.
  ✷ ENCRYPTION ON ALL ENDPOINT DEVICES.

DATA BREACH EXAMPLES (CONT)

✓ POOR SECURITY...
  ✷ MADE KNOWN – JAN 2017
  ✷ SWEDISH TRANSPORT AGENCY – "KEYS TO THE KINGDOM"
  ✷ INFORMATION ABOUT ALL VEHICLES IN THE COUNTRY – INCLUDING POLICE AND MILITARY – WAS MADE AVAILABLE TO IT WORKERS IN EASTERN EUROPE
  ✷ OUTSOURCED IT MAINTENANCE WITHOUT PROPER SECURITY CLEARANCE CHECKS
  ✷ ADMINISTRATORS IN THE CZECH REPUBLIC WERE GIVEN FULL ACCESS TO ALL DATA AND LOGS
  ✷ IT IS NOT KNOWN WHETHER THE SECURITY GLITCH CAUSED ANY MAJOR DAMAGE

DATA BREACH EXAMPLES (CONT)

✓ PREVENTION...
  ✷ FULLY VET ALL YOUR VENDORS AND UNDERSTAND HOW THEY WILL HANDLE YOUR DATA
  ✷ ASSIGN DATA ACCESS PRIVILEGES APPROPRIATELY
WHERE ARE WE GOING?

✓ CLOUD SOLUTIONS ARE CATCHING ON IN HEALTHCARE
  ◆ CLOUD SYSTEMS TO MANAGE AND EXCHANGE DATA ARE ON THE RISE
  ◆ ANALYTICS HAS BEEN ON THE RISE – 3RD PARTY CLOUD SYSTEMS

WHERE ARE WE GOING?

✓ ISSUES...
  ◆ SHARED SECURITY MODEL
  ◆ INFORMATION BEING TRANSPORTED AND STORED – WHERE IS IT?
  ◆ NEW POTENTIAL POINTS OF FAILURE IN SECURITY PROCESS – LEARNING CURVE

WHERE ARE WE GOING?

✓ OLD FRIENDS GETTING MORE PREVALENT (PHISHING AND RANSOMWARE)
  ◆ RANSOMWARE AS A SERVICE –
    ▶ DEVELOPED BY MALWARE AUTHORS THEN DISTRIBUTED TO OTHER CRIMINALS TO TAKE PART IN ATTACKS VIA THE DARK WEB
    ▶ THE MAIN DEVELOPER GETS A CUT OF THE ACTION FOR SUCCESSFUL RANSOM PAYMENTS
    ▶ USE OF PORTALS TO DEPLOY AND TRACK THE RANSOMWARE
WHERE ARE WE GOING?

✓ RANSOMWARE AS A SERVICE (EXAMPLES) –
  ◆ GRANDCRAB
  ◆ SATURN
  ◆ DATA KEEPER
WHERE ARE WE GOING?

✓ COIN MINING IS CATCHING ON
  ◆ CRYPTOCURRENCIES ARE DIGITAL CURRENCIES: THEY ARE CREATED USING COMPUTER PROGRAMS AND COMPUTING POWER, AND RECORDED ON THE BLOCKCHAIN.
  ◆ TO CARRY OUT THIS ACTIVITY COMPUTING RESOURCES ARE REQUIRED: GOTTEN ON WEBSITE VISITS OR RUNNING IN BROWSERS.
  ◆ NOT ILLEGAL AND VALID WAY TO PAY FOR WEBSITE USAGE = MUST BE DISCLOSED

WHERE ARE WE GOING?

✓ COIN MINING IS CATCHING ON
  ◆ CYBER CRIMINALS SURREPTITIOUSLY INSTALL MINERS ON VICTIMS' COMPUTERS OR INTERNET OF THINGS (IOT) DEVICES WITHOUT THEIR KNOWLEDGE.
  ◆ COINHIVE IS A CRYPTOCURRENCY MINING SERVICE THAT RELIES ON A SMALL CHUNK OF COMPUTER CODE DESIGNED TO BE INSTALLED ON WEB SITES. (MONERO CRYPTOCURRENCY)
WHERE ARE WE GOING?

✓ INTERESTING STATS ON IOT

❖ An estimated 2.5 billion devices will be connected to the Internet by 2021, up from 6 billion in 2016. Total spending on IT, including data center systems, enterprise software and connected devices is expected to reach $4 trillion in 2021, up from $3.4 trillion in 2015.

WHERE ARE WE GOING?

✓ INTERESTING STATS ON IOT

❖ IOT budgets are set to rise an average of 34% over the next 12 months, and the most notable beneficiaries will be these vertical industries: B2B software and services (leading at +41%), manufacturing (+37%), healthcare (+28%) and utilities (lagging at +26%).

ADDRESSING THE THREATS

CYBERSECURITY FRAMEWORK – DEFINITION

✓ The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks. It “provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.”
**ADDRESSING THE THREATS**

**DATA LOSS PREVENTION (DLP) – DEFINITION**

*DATA LOSS PREVENTION (DLP) IS A SET OF TOOLS AND PROCESSES USED TO ENSURE THAT SENSITIVE DATA IS NOT LOST, MISUSED, OR ACCESSED BY UNAUTHORIZED USERS.*

* digitalguardian.com

**ADDRESSING THE THREATS**

**DATA LOSS PREVENTION (DLP)**

*ISACA’S DATA LEAK PREVENTION WHITE PAPER IDENTIFIES THREE KEY OBJECTIVES FOR A DLP SOLUTION:*

- LOCATE AND CATALOG SENSITIVE INFORMATION STORED THROUGHOUT THE ENTERPRISE. (IDENTIFY)
- MONITOR AND CONTROL THE MOVEMENT OF SENSITIVE INFORMATION ACROSS ENTERPRISE NETWORKS. (DETECT)
- MONITOR AND CONTROL THE MOVEMENT OF SENSITIVE INFORMATION ON END-USER SYSTEMS. (PROTECT)*

* digitalguardian.com

---

**ADDRESSING THE THREATS**

**CYBERSECURITY FRAMEWORK – NIST**

<table>
<thead>
<tr>
<th>Control Area</th>
<th>Control</th>
<th>Category</th>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST 800-50</td>
<td>Network Policy</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Network Security</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>System Security</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Application Security</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Data Security</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Security Assessment</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Security Authorization</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Security Controls</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Security Controls</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
<tr>
<td>NIST 800-50</td>
<td>Security Controls</td>
<td>Security</td>
<td></td>
<td>Support Information Security and Privacy</td>
</tr>
</tbody>
</table>

*Created by Security Assurance LLC, 2018*
ADDRESSING THE THREATS
DATA LOSS PREVENTION (DLP)

✓ THE WHITE PAPER PROVIDES GUIDELINES FOR IMPLEMENTING DLP. THESE GUIDELINES ARE:

✓ DATA CLASSIFICATION SHOULD BE THE FIRST STEP OF THE PROGRAM.
✓ DEFINE AND IMPLEMENT DATA CLASSIFICATION AND PROTECTION POLICIES.
✓ IMPLEMENT AND CONFIGURE DLP SOLUTIONS PER POLICY.
✓ IDENTIFY AND MONITOR THE RISK ASSOCIATED WITH LIMITATIONS OF DLP SOLUTIONS IN PROTECTING THE ORGANIZATION’S DATA.

ADDRESSING THE THREATS
DATA LOSS PREVENTION (DLP)

✓ THREE PRIMARY STATES OF DATA ARE:

✓ DATA AT REST (ID, LOCATE, LOG)
✓ DATA IN MOTION (MONITORING NETWORK TRAFFIC)
✓ DATA IN USE (ENDPOINTS)

ADDRESSING THE THREATS
BUSINESS BENEFITS OF DLP

✓ PROTECT CRITICAL BUSINESS DATA & INTELLECTUAL PROPERTY
✓ IMPROVE COMPLIANCE
✓ REDUCE DATA BREACH RISK
✓ ENHANCE TRAINING & AWARENESS
✓ IMPROVE BUSINESS PROCESSES
✓ OPTIMIZE DISK SPACE & NETWORK BANDWIDTH
✓ DETECT ROGUE/MALICIOUS SOFTWARE