LIVING A SECURITY BREACH

Setting ourselves up for failure

PRE-BREACH

Cultural Bias

- Growth and revenue focused
  - Profits pushed back into fiber builds and network rollout
- The Customer was #1
  - Customer capture and satisfaction, prioritized over everything else
- We believed we were not a target
  - We were small
  - We didn’t hold Personally Identifying Information (PII)*
  - We had no Credit Card transactions

Cultural Bias

- We believed we had adequate IT measures
  - We relied on passwords as a protection
  - We trusted Microsoft for security patching
  - We trusted our employees to do their part
    - To update their passwords and virus protection
    - To be diligent, savvy, and aware
- We approached IT security as the prevention of threats

THE BREACH

Walking through the door

- October 2018
  - Emotet virus picked up by an employee visiting the web while working from home
  - Elevated privileges used by IT person debugging employees machine lets the virus into the LAN
    - LAN was heavy Windows based servers, PCs, etc. and virus spreads within minutes
    - The virus was believed contained and no trace could be found via Windows supplied Antivirus SW
- November was quiet

Walking through the door (Cont.)

- December 2018
  - CenturyLink takes a major hit
    - We meet internally to discuss, and decide (without any supporting evidence), that they were hacked
  - We decide on steps to beef up our defenses
    - But our cultural bias tempers our urgency
  - Two Factor Authentication(2FA) ordered for servers
    - Added as a background task for IT
  - Email migration to a hosted platform begins
    - Delayed by resistant employees
- January was quiet

Wednesday Feb 6th, 2019

- At 4:15am my cell phone rings and my IT manager reports;
  - At 1:00 am, a ransomware event starts encrypting our servers
  - By 1:45 am, the attack had been stopped but the damage was extensive
  - A significant bitcoin ransom was demanded by the group known as RYUK
- The first question I remember asking was….is our customer facing network up?

Wednesday Feb 6th (Cont.)

- Directive 1…mobilize IT and Engineering
- Directive 2…under no circumstance is anything to be rebooted/turned off
- By 5:30 am we had a war room set up and all applicable staff working to;
  - Assess the damage
  - See if we could work our way out of it
- I remember looking at the uninstalled 2FA fobs in the IT managers office

Wednesday Feb 6th (Cont.)

- By noon it was clear it was an orchestrated attack with no recovery
  - We had no email except for those few that had been moved to the hosted platform in December/Jan
  - 50 servers were attacked simultaneously and frozen
  - All Windows based systems were inaccessible except for the domain controller that was being used to execute the attack
  - The Linux and Mac environments were untouched
  - We had no access to files, no business applications, and no Element Management System (EMS) level network visibility

Wednesday Feb 6th (Cont.)

- We contacted the FBI…they were no help
- We contacted our cyber insurance carrier
  - "We do 15 of these a week and you're covered"
  - They put us in contact with an attorney and cyber security firm for consultation
- We spent the rest of Wednesday assessing the damage in order to decide if we wanted to pay the ransomware
- I contacted my Board of Directors and would do so each day until the crisis was over

Thursday Feb 7th

- We put a plan in place for recovery and communicated it to key, but not all, employees
  - SNMP network visibility was priority 1
  - Hosted Email was priority 2
- We made the decision to pay the ransom and started the process
  - Our General Counsel and Director of Finance took lead
- Prior to getting the key, we began rebuilding some servers on existing host machines and moved most others to the Cloud

Friday Feb 8th – Sunday Feb 9th

- Friday all employees came into the office
  - They had nothing to do but feel the pain of a situation they helped create
  - Our parking lot was full, signaling business as usual to all by-passers
  - We set up a “recovery status” board
- Due to complications with a third party we were not able to pay the ransom until Sunday morning
- Enough business applications were up by Monday to return to work in a diminished capacity

Lessons Learned

POST BREACH

The Impact Continues

- We are still recovering from the breach
- We had to drive home the fact that we were not recovering to where we were…..*that we were recovering to where we needed to be*
- We found continuing presence of Emotet inside our LAN 45 days after the initial attack
- We found our corporate data for sale on the dark web

Cultural Change

- We are willing to slow growth in order to protect our IT integrity
- The Customer is still #1
- We know we are, and forever will be, a target
- We know we will never have enough security measures
  - We no longer rely on passwords as a protection
  - We do not trust Microsoft to do their part in security patching

Cultural Change (Cont.)

- We do not depend upon employees to do their part
  - Updates are pushed
  - Employees are locked out for security policy breaches
  - We use 2FA on almost everything
    - email, server access, business applications, Amazon, etc.
  - We use real-time 3rd party anti-virus
  - We use very aggressive content filtering on web access
  - All PCs are being reviewed for replacement with employees being moved to an iPad first, then Mac, and as a last resort, a Windows based machine
  - Private Key Exchange from certificate authority for VPN

Final Word

WE NOW APPROACH IT SECURITY AS THE CONTAINMENT OF THREATS (*INCLUDING EMPLOYEES*), INSTEAD OF THE PREVENTION OF THREATS