CYBER INCIDENT RESPONSE

The Secret Service Perspective

– Kevin McCleary & Abigail Tyrrell

CREATE
test attacks
Best Practices
MOVE SLOW
DELEGATE
Vulnerabilities
LOOK For OPEN PORTS
RESEARCH TARGETS
Admin Rights
HIGH VALUE
Evidence
Disrupt and dismantle criminal threats in a meaningful way
HISTORICAL DATA
HIGH VALUE
Targets
HUMAN intelligence
APPROACH
USSS USSS
DATA BREACHES
40% of comes from
MALWARE
EMAIL
Hard to Cross Out of the Problem
76% Financially MOTIVATED
LAW ENFORCEMENT
ROLES: Discover VICTIMS
COLLECT INFO
RESPOND WITH RESILIENCY
provide info to network defenders
ACTIONABLE
YOU WILL NEVER BUILD A BULLET PROOF SYSTEM
EARLY DETECTION IS KEY
WHY EVEN THE BEST PRACTICES FAIL
HUMAN NATURE + LAZINESS
COMPLEX
NYCFE.org
physical protection
INTEGRATED MISSION
financial protection
TODAY'S ROBBERS:
WHY DO YOU ROB? BANKS
HACK
THAT'S WHERE THE MONEY IS AT.
INFORMATION
VICTIMS:
45% SMALL BUSINESSES
16% PUBLIC SECTOR
HEALTH SECTOR
15%
16% financial SECTOR
•Review
•your
•Logs
White list Applications
email compromise
COVID-19 SCHEMES
TRENDING Cyber CRIMES
social media scams
RANSOMEWARE
HAVE A RESPONSE PLAN
Review & Test
Skimming
ESTABLISH CONTACTS
Coordinate With Law Enforcement
HACKERS ONLY HAVE TO BE RIGHT ONCE
PASSWORDS
MUTI-FACTOR AUTHENTICATION
Sharing
NFO is KNOWLEDGE
Sharing
Cyber Fraud Task Force
CFTF
INFO SHARING
RESPONSE PREVENTION
FOCUS ON CRIME
WHO?
IS BEHIND THE BREACHES
STEAL INFORMATION For Financial Gain
69% OUTSIDERS
39% CRIMINAL GROUPS
33%
Social Attacks
52% HACKS
INVOLVED MALWARE
28%