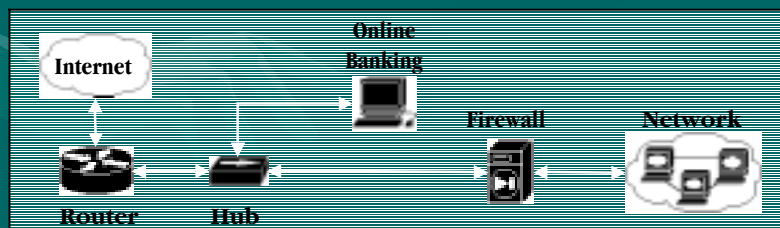


Security An Everyday Activity

George Richardson
Security State Bank

Introduction

- ◆ Security State Bank located in Littlefield Texas
- ◆ Deployed online banking solution September 1997
- ◆ 3rd bank with Z Corp for online banking software
- ◆ Router with Access Control List protecting online banking server and firewall to protect internal network.
- ◆ Web banking server ran using initial install configuration for almost three years



Monday Morning Wake Up Call

◆ Not the way to start your Monday

From: Bank Banking [bank-ru@doctor.com]
Sent: Monday, April 10, 2000 4:51 PM
To: grichardson@security-state-bank.com
Subject: Secure is BAD
Hello George Richardson!
Secure on ur site is bad. All "hackers" read all information about ur clients, and run transaction... eg:
XXXX Checking \$11,424.09
XXXX-001 Checking \$109,784.34
XXXX Savings \$285.58
YYYY2 Loan (11.000% Due 02/01/02) \$4,930.90
YYYY7 Loan (11.000% Due 02/01/02) \$14,272.32
YYYY5 Loan (10.500% Due 02/15/05) \$37,571.53
YYYY6 Loan (10.000% Due 03/01/03) \$10,907.05
YYYY2 Loan (11.000% Due 11/20/00) \$2,023.06
YYYY2 Loan (10.000% Due 03/01/03) \$28,882.61
YYZZ1 Loan (9.000% Due 03/01/05) \$52,000.00
and over.....
if interested more information - plz send me e-mail =)
Best regards, Aleksandr

What We Did Right

- ◆ Contacted Z Corp within the hour.
- ◆ Contacted the FBI
- ◆ Contacted the regulators
- ◆ Filed an SAR
- ◆ Had our network consultant on site within an hour.
- ◆ Protected the scene for forensics
 - ◆ Did not power down server
 - ◆ Did not start looking at files or logs on the server
 - ◆ Took server offline to the public
- ◆ Contacted trusted sources for outside security consulting recommendations
- ◆ Implemented corrective procedures

What We Did Wrong

- ◆ Did not originally ensure that the web server was hardened before putting that server online
- ◆ Did not deploy full firewall feature set on router.
- ◆ Did not fully understand the difference between our duties and the duties of Z Corp.
- ◆ Underestimated the attractiveness of hacking a small bank located in Littlefield
- ◆ Assumed someone else would administer security patches and hotfixes
- ◆ Did not have a daily evolving security mindset.

What We Learned

- ◆ Compromise came from a published vulnerability with IIS 4.0 that had a hotfix available for over one year
- ◆ Most system compromises are the result of published vulnerabilities that haven't been patched
- ◆ Question all software vendors deploying software or hardware onto network.
 - ◆ What ports are required (opened), do they require internet access
 - ◆ Who maintains patches and deploys hotfixes, etc
 - ◆ Review vendors security policies, after implementation, check it out!
- ◆ Involve network consultants in software and hardware deployments
 - ◆ They can evaluate the effectiveness of the product
 - ◆ They can access how the product will work on the network

What We Learned – Continued

- ◆ Implement documentation procedures
 - ◆ Document applications of upgrades, patches, and hotfixes
 - ◆ Document review of logs
- ◆ Implement multiple layers of security defense
 - ◆ Firewalls
 - ◆ DMZs
 - ◆ Intrusion Detection Systems (IDS)
- ◆ Employee training on security policies and safe computer use
- ◆ Must have management and board commitment to security

How Our Network Has Evolved

- ◆ Our basic network five years ago consisted of a firewall running Access Control List blocking major protocols used for attacks
- ◆ Network security is a work in progress
 - ◆ Vendor review and assessment
 - ◆ Multiple firewall deployment
 - ◆ Multiple IDS systems (external and internal) using different vendors
 - ◆ Scanning of email
 - ◆ User authentication to access the internet
 - ◆ User authentication to access network resources
 - ◆ Multiple DMZ zones
 - ◆ 3DES encryption

How Our Network Has Evolved Continued

- ◆ Logging, change logs, internet usage logs, server logs
- ◆ Virus software and pattern update compliance logs
- ◆ Security update and hotfix installation logs
- ◆ Network scan comparison logs
- ◆ IDS to monitor system files
- ◆ Monitoring of network resources
- ◆ Use of outside consultants for verification, feedback and audit