Siku Njema! – Good Day!
Defense In-depth Security Approach

SECTION 1
Introductions

SECTION 2
The Wild Wide Web

SECTION 3
Cyber Breaches - Causes

SECTION 4
Case - Study

SECTION 5
Defense In-depth Approach

SECTION 6
Questions
IS was founded in 1993. It is an Internet Protocol Communication's Service Provider on the African Continent and a subsidiary of Dimension Data.
SEACOM is a submarine cable operator with a network of submarine and terrestrial high-speed fibre-optic cable that serves the east and west coasts of Africa. SEACOM’s reach extends into Europe and the Asia-Pacific via India.
As of June 2017, 51% of the world's population has internet access.
<table>
<thead>
<tr>
<th>Threat</th>
<th>Period</th>
<th>Response Time</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt; Gen – Boot Virus</td>
<td>The 80's</td>
<td>Weeks</td>
<td>Individual PC's</td>
</tr>
<tr>
<td>2&lt;sup&gt;nd&lt;/sup&gt; Gen – Macros Viruses and DoS</td>
<td>The 90's</td>
<td>Days</td>
<td>Individual Networks</td>
</tr>
<tr>
<td>3&lt;sup&gt;rd&lt;/sup&gt; Gen</td>
<td>DDoS &amp; Mixed threats</td>
<td>Minutes</td>
<td>Multiple Networks</td>
</tr>
<tr>
<td>4&lt;sup&gt;th&lt;/sup&gt; Gen</td>
<td>Flash threats, Massive “bot” – driven DDoS &amp; Damaging payload worms</td>
<td>Seconds</td>
<td>Regional Networks &amp; Global Infrastructure.</td>
</tr>
<tr>
<td>Current</td>
<td>Dark-web; Ransomware</td>
<td>Immediately</td>
<td>ALL</td>
</tr>
</tbody>
</table>
Cybercrime

Criminal activities carried out by means of computers or the Internet.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cyberbullying</td>
</tr>
<tr>
<td>2.</td>
<td>Cyberterrorism</td>
</tr>
<tr>
<td>3.</td>
<td>Cyberextortion</td>
</tr>
<tr>
<td>4.</td>
<td>Cyberwarfare</td>
</tr>
<tr>
<td>5.</td>
<td>Financial Fraud</td>
</tr>
<tr>
<td>6.</td>
<td>Fraud and Identity theft</td>
</tr>
<tr>
<td>7.</td>
<td>Information Warfare</td>
</tr>
<tr>
<td>8.</td>
<td>Phishing Scams</td>
</tr>
<tr>
<td>9.</td>
<td>Spam</td>
</tr>
<tr>
<td>10.</td>
<td>Offensive/Obscene Content</td>
</tr>
<tr>
<td>11.</td>
<td>Drug Trafficking – Darknets</td>
</tr>
<tr>
<td>12.</td>
<td>Computer Viruses</td>
</tr>
<tr>
<td>13.</td>
<td>DDoS/DoS</td>
</tr>
<tr>
<td>14.</td>
<td>Malware</td>
</tr>
</tbody>
</table>
Sources of Threats – Anywhere

**The Internet**
Downloading malicious software disguised as keygens, cracks, patches or downloading files via peer-to-peer networks (for example, torrents).

**Email**
Spam and Phishing

**Software Vulnerabilities**
Vulnerabilities, bugs and glitches of software grant hackers remote access to your computer

**Removable data storage media**
When you run a file from a removable media you can infect your computer and spread the virus to the drives of your machine.
Sources of Threats – Anywhere

**User Actions**
Using various tricks, malefactors make users install their malicious software. Insider Threats

**Network Vulnerabilities**
Allows hackers to take over entire domains (pharming)

**Improper Configurations**
Through Improperly configured firewalls and legacy firewall technology

Internet Solutions is a division of Dimension Data
Case Study.

2017 Ransomware Attacks

Months Running to September 2017 the whole Internet was on high Alert due to Ransomware attacks.

Ransomware – malware that threatens to block (encrypt) access or infringe on data privacy unless a ransom is paid. Common mode of attack is through Trojans.

The Ransom is paid through the use of digital currencies making it difficult to trace the attacker. Payments are not guarantee of Decryption. Most recent notable attacks were WannaCry, Petya and Bad Rabbit.

Threat E-mail to Customer – DDoS Warning

One of our customers engaged us after receiving a threat Email whose magnitude meant financial loss and reputation damage.
**Case Study.**

Months Running to the Month of September 2017 the whole Internet was on high Alert due to Ransomware attacks.

2017 Ransomware Attacks

One of our customers engaged us after receiving a threat Email whose magnitude meant financial loss and reputation damage.

**Threat Email – DDoS Warning**

Internet Solutions is a division of Dimension Data

19 September 2017 at 19:04

- uid101080@web.webs...

Hello, [removed]

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Phantom Squad

Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 Bitcoin @ [removed].

If you don't pay by Sept 30st 2017, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

This is not a joke.
Case Study.

Months running to the month of September 2017 the whole Internet was on high alert due to Ransomware attacks.

2017 Ransomware Attacks

One of our customers engaged us after receiving a threat email whose magnitude meant financial loss and reputation damage.
Case Study - Old Security Techniques
Case Study - Old Security Techniques

1. Everyone on the Internet is a suspect
2. Everyone within my organization is trustworthy
3. Security model built to lock outsiders
4. Hosts were protected with AV only and Firewall was everything!
5. Monitoring did not exist
6. Limited or no internal segmentations
Case Study - Defense In-depth Approach

1. Establishing the authenticity of the threat E-mail
2. Vulnerability and Penetration testing on client network
3. Quick work-arounds + Patch Management System
4. Deployment of Disaster recovery site and Activating our NOC/SOC Team
5. Cloud Scrubbing Phase
6. Review of Internal Processes and Policies
Case Study – Defense In-depth Approach

- **Identify**
  - Assessment
  - Exploit?
  - Alerts
  - Compliance

- **Analyze**
  - Measure
  - Profile
  - Classify
  - Impact

- **Mitigate**
  - Respond
  - Contain
  - Remediate
  - Implement

- **Manage**
  - Baseline
  - Correlate
  - Prevent
  - Integrate
Case Study – Defense In-depth Approach
Case Study – Defense In-depth Approach
<table>
<thead>
<tr>
<th></th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Breach Detect – Honeypots</td>
</tr>
<tr>
<td>2</td>
<td>Manage User access to web content – accepted policies (Cloud Web Security)</td>
</tr>
<tr>
<td>3</td>
<td>Disaster recovery site + Cyber Insurance</td>
</tr>
<tr>
<td>4</td>
<td>DDoS Protection</td>
</tr>
<tr>
<td>5</td>
<td>DNS Url Filtering</td>
</tr>
<tr>
<td>6</td>
<td>Next-Gen Firewalls - Managed Firewall service</td>
</tr>
</tbody>
</table>
Case Study – Resolves Made

7. IPS – IPS software is continually updated with new signatures

8. PhishNet – Inhouse Phishing Campaign

9. Secure Connect – Send Data Safely – Multi-authentication

10. Vulnerability Scanning + Patch Management + Internal Audits

11. Web Application Firewalls & Email Security

12. Penetration Testing – PCI Compliance
Success in Defense In-depth Approach

Results

1. We were able to track the source of e-mail
2. We were not keen on taking legal action due to cross border legislations - but used postmaster account to report the offending host
3. We move into blacklisting and null routing the suspected source
4. Amplification and Volumetric attacks though not major were stopped at the perimeter (cross-connect) before reaching customer network
5. We continued helping the customer in reviewing internal processes and procedures.
6. Our customer took up key services from us – having confidence on our delivery capabilities
Contact Us

We want to hear from you. Get in touch with us
www.is.co.ke/contact-us/

PHONE
+ 254 20 360 0200

EMAIL
info@is.co.ke

WEBSITE
www.is.co.ke