Global vision.
Local knowledge.

Cisco Connect Dubrovnik
Croatia • 28.03.2019
Cisco Email Security

Zaštitite svoj najosjetljiviji dio sustava od napada

Vedran Franjić
System Engineer Sales
29.03.2019.
Agenda

• Email importance
• Multilayer approach
• DP and APP
• Securing o365
• Architecture
• Intelligence
• Licensing
Email Importance
Figure 3: Secure Email Gateway Market Quadrant, 2018*
Grad uplatio prevarantu 50.000

R.I.
15.9.2018.

NEKOLIKO tvrtki i institucija u Hrvatskoj dobilo je tijekom srpnja lažne mailove u kojima ih se traži da na inozemni račun uplate veće iznose.

Pročelnik za financije Grada bio je jedan od njih. 9 srpnja dobio je e-mail u kojem gradonačelnik od njega traži da izvrši hitnu uplatu na bankovni račun naveden u mailu. Pročelnik je s računa Grada prebacio 50.000 eura na navedeni račun.

"U Odjelu za financije stigla je poruka s upitom možemo li obaviti plaćanje u inozemstvo. Počinatelj prijave u zabluđu je doveo našeg službenika tako što se predstavio u moje ime, napravio lažni mail i podacima kao da sam to ja", objašnjava gradonačelnik. Počinatelj mu nije hakirao mail, nego adresu s koje je poslao svoj mail nazvao gradonačelnikovim imenom. "Na taj mail pročelnik je odgovorio upitom na koji račun, komu i koji iznos, provjerio u banci može li ići uplata, dobio instrukcije za plaćanja i ono je odrađeno", objašnjava za Glas Slavonije gradonačelnik.

Podsjecačući na proceduru kako se obavljaju plaćanja, dodaje kako se taj dan, do tada, on i pročelnik nisu vidjeli ni čuli. Oko 14.30 sati, nastavlja, pročelnik mu na mail šište potvrdu o uplati.

*Bišo mi je malo čudno. Prvo se činilo da je nama netko nešto platio iz Britanije, no potom vidim da smo mi..."
Email was not built with security

It’s easy for attackers

95% of breaches start with email
Attacked Use **Multiple Ways** to Get In

Malware

- Ransomware detections up 90% in 2018\(^1\)

Business Email Compromise (BEC)

- $5.3 Billion in losses\(^2\)

Phishing

- $9.1 Billion in 2018\(^3\)

Domain Compromise

- 54% of legitimate domains used in phishing campaigns\(^4\)
Multilayered Approach
Team,

At Cisco, it’s our mission to design secure products. Now it’s your mission to protect data and assets belonging to Cisco, our customers, and our partners from threats lurking around every corner.

Engage now: http://thislinkisagiantscam.youresilly.cisc0.com/swag

It’s times like these when it is critical that we come together, support each other, and have each other’s backs.

Thank you,

John
Protect personal information and IP
Data Loss Prevention (DLP)

Control what leaves the network and customize policies
Scan email content for sensitive information
Prevent data exfiltration automatically

Manage policies such as:
• Specific users
• Groups
• Locations
• Federal compliance
• State regulations
With multi-language support

Cisco Email Security

Critical violation: Info redirected and not sent
Minor violation: Content sent with encryption
No violation: Content sent with optional encryption

Scanned against 100+ predefined DLP policies
Extend security to external communications
Cisco Registered Envelope Service (CRES)

Scan messages for keywords, policies, and sender
Apply authentication mechanisms to access encryption keys
Maintain control over your sent messages
DP and APP
Advanced phishing attacks use identity impersonation

- Content Deception
- Identity Impersonation

Volume of Threats

- Zero Day Attacks
- Social Eng Attacks
- Spear Phishing
- Business Email Compromise

- Spam
- Email Malware

2000s 2015 2017

30% open malicious emails
13% click on malicious attachments
3:45 until first user is compromised

Sources: CSOonline.com, Cybersecurity ventures, Nucleus Research, FBI I3C (Jan ’15 – Dec ’16)
Block fraudulent senders

DMARC, DKIM and SPF

- **DMARC**: Ties SPF and DKIM results to 'From' header
- **DKIM**: Matches public key to sender domain's private key records
- **SPF**: Checks if mail from a domain is being sent from an authorized host

Determine whether a sender is reputable

Inspect sender details on inbound messages

Block invalid senders and identify next steps
$ telnet alln-mx-01.cisco.com 25
Trying 173.37.147.230...
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-e.cisco.com ESMTP
  helo pipershark.com
  250 alln-inbound-e.cisco.com
MAIL FROM:<admin@pipershark.com>
  250 sender <admin@pipershark.com> ok
RCPT TO:<robsherw@cisco.com>
  250 recipient <robsherw@cisco.com> ok
DATA
354 go ahead
Subject: SMTP CONVERSATION TEST MESSAGE
From: Email Admin <admin@pipershark.com>
To: Robert Sherwin (robsherw) <robsherw@cisco.com>
Here is the email, hope you receive it.
.
250 ok: Message 143004492 accepted
quit
221 alln-inbound-e.cisco.com
Connection closed by foreign host.
DMARC, DKIM and SPF

dhs.gov IN TXT "v=spf1 ip4:216.81.91.184 ip4:216.81.85.157 include:spf.protection.outlook.com -all"

Algorithms used
- DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
  d=ietf.org; s=ietf1;
  h=To:From:Subject:List-Id:List-Unsubscribe:List-Archive:
  List-Post:List-Help:List-Subscribe;
  bh=+IImGr4kx/dTzpOOk1mcWyVJTzHFzo8kD6dIgqvZvk2qY=;
  b=DmDxUN1XbQTWb99003VdnQn5ntUmK6kvF6Iu/ZFmIHjoo/r5b85Cu8u4x
  H1ZF2gh664WyOb2ffYJ9bcfwb3JvTv6d3bndL8/bvYtOXUR7g1MqMc32Zn/d60
  pXWbQa16+ZW6KwwWF+mDlhpztNwFsG6oRprDLUuzBSupVx7s74=

Version Failure policy Sampling rate
_dmarc.amazon.com IN TXT "v=DMARC1; p=quarantine; pct=100;
rua=mailto:dmarc-reports@bounces.amazon.com;
ruf=mailto:dmarc-reports@bounces.amazon.com"
Email Authentication Overview

**SPF**
- Authenticates Message Path
- Authorized senders in DNS

**DKIM**
- Authenticates Message Content
- Public Encryption keys in DNS

**DMARC**

- **Reliable**
- **Visibility**
- **Action-Based Policies**
- **RUA**
- **RUF**
Forged Email Detection
FBI defines it as Business Email Compromise (BEC)

Pre-processing

From: Chuck <chuck.robbins@mail.com>
Subject: [URGENT] Need help transferring funds

Inspect SMTP envelope address:
$ telnet smtp-in.l.mail.com 25
Trying 74.125.206.26...
Connected to smtp-in.l.mail.com.
Escape character is '^]'.
220 mx.mail.com ESMTP i11si22058766wmh.67 - gsmtp
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM:<adam@outside.com>
250 2.1.0 OK i11si22058766wmh.67 - gsmtp
RCPT TO:<alan@mail.com>
250 2.1.5 OK i11si22058766wmh.67 - gsmtp
Data

Sending Domain

Actual Sender

Recipient Domain

Send appended mail to warn users of potential forgery

Post-processing

From: adam@outside.com
Subject: {Possibly Forged} [URGENT] Need help transferring funds

Inspect SMTP envelope for True sender address

Match sender address against company directory

Record a log of attempts and actions taken
Protect your brand
Cisco Domain Protection

- Easily analyze, update and take action against those misusing your domain to send malicious email
- Validate those who use your domain appropriately

Automate DMARC authentication
- Drive to DMARC Enforcement with proven tools and services

Block attackers from using your domain
Protect against fraudulent senders

Advanced Phishing Protection

Local intelligence

- Learns and authenticates identities and behavioral relationships for enhanced protection

Reduce business email compromise

- Discerns which emails carry targeted phishing attacks and only legitimate emails get delivered
Message Details

Date: 5-Mar-2019 14:13:57 AEDT

From: Ada Stevesty <Ada.Stevesty@mastercard.com>

To: Handrista.Kacelith@ciscofunding.com

Subject: Your PG&E Energy Statement is Ready to View

Message ID: <facade06a00406e3e887349eb7569d38@BY2PR12MB80054.mastercard.com>

Message Trust Score: 0.3 (Untrusted)

- Look-alike Domain
  mastercard.com is an imposter of mastercard

- Individual Display Name Impostor
  Ada.Stevesty@mastercard.com is an imposter of ada stevesty

Matched policies: [QUAR] Untrusted Messages

Look-alike Domains

Message Trust Score Reasons

- Authenticity Score: 0.1
  Very low Authenticity Score

  MAIL FROM: △ MAIL FROM does not match Header From: domain

  DKIM 'd=' tag: Not available

  Authentication results:
  △ SPF result not reported
  △ DKIM result not reported
  Unknown

Sending Domain: mastercard.com
Domain Reputation: 0.6
  Frequent, High Volume Sender

Sending IP Address: 52.24.169.89 — (ec2-52-24-169-89.us-west-2.compute.amazonaws.com)
SBRS: Not available

Search for similar messages
Secure o365
<table>
<thead>
<tr>
<th>O365 – E3</th>
<th>Cisco Email Security w/O365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-spam filters</td>
<td>Anti-spam filters</td>
</tr>
<tr>
<td>Anti-virus protection</td>
<td>Anti-virus protection*</td>
</tr>
<tr>
<td>Policy enforcement</td>
<td>Policy enforcement</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>Disaster recovery</td>
</tr>
<tr>
<td>Directory services</td>
<td>Directory services</td>
</tr>
<tr>
<td>Advanced Threat Protection (Safe Links, Safe Attachments)*</td>
<td>Graymail detection</td>
</tr>
<tr>
<td>Message tracking (limited)</td>
<td>Outbreak Filters</td>
</tr>
<tr>
<td>Email encryption (cloud-based only)</td>
<td>Message tracking</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>Email encryption (cloud and on premise)</td>
</tr>
<tr>
<td>Advanced Malware Protection</td>
<td>Advanced Malware Protection</td>
</tr>
<tr>
<td>Detailed reporting</td>
<td>Detailed reporting</td>
</tr>
<tr>
<td>Zero-day incident management</td>
<td>Zero-day incident management</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>Data loss prevention</td>
</tr>
</tbody>
</table>

*Anti-virus provided by O365
*Only with E5
Easily Integrate with Office 365

O365 Exchange Online

Cisco Email Security

Inbound Traffic

Outbound Traffic
4. No Quarantine Policy, Email Delivered

Azure Application Permissions:
- Send mail as any user
- Read and write mail in all mailboxes
- Read mail in all mailboxes
- Full access to all mailboxes

6. Remediation (all mailboxes)

AMP Retrospective Event Flow:
1. Email with attachment arrives
2. File Reputation Query (SHA256)
3. AMP Verdict: OK
4. AMP Retrospective Verdict Update: Malicious
Cisco Threat Analyzer For o365

A free assessment tool to identify security gaps

Visibility into threats gone undetected

Summary scan report with details
Once the ‘Scan Completed’ is shown

Review the Dashboard, compile the PDF report, and share the report with the customer.
Arhitecture
Don’t compromise on features when making a choice

- Cloud
- On-Premises (Physical or Virtual)
- Hybrid
- Cluster
Transition to the cloud with confidence

Cisco Email Security

- Integrate easily with O365
- Deliver 99.999% availability
- Prevent shared-fate with compute instances
- Increase dedicated instances up to 50% at no cost
- Migrate to new deployment options easily
CES: New Datacenters

4 new DCs launched in:
- Toronto
- Kamloops
- Oregon (AWS)
- N. Virginia (AWS)

Additional sites:
- Switzerland
- Germany
- Australia (x2)
- Japan
- Singapore

- 99.999% Uptime Guarantee
- Geo-Redundant Clusters
- Choice of DC location
Threat Intelligence
The Foundation: Superior Threat Intelligence from Cisco Talos

Visibility across all vectors from a best in class portfolio
The Foundation: Cisco Talos Continued

1.5M
New daily malware samples

600B
Daily email messages

16B
Daily web requests
Talos on Cisco Email Security

Monitors 600 billion emails per day to provide more broad visibility

Sender Analysis  Content Analysis  File Analysis  URL Analysis
Licensing
Product Offering: Licensing

• 1. Choose deployment
  ESA, vESA, CES

• 2. Choose Bundle
  Inbound:  Anti-spam + Virus + Outbreak filters
  Outbound: Data Loss Prevention + Encryption
  Premium: Inbound + Outbound

• 3. Choose add-on
  AMP – Advanced Malware Protection
  GSU – Graymail Safe-Unsubscribe
  DP – Domain Protection
  APP – Advanced Phishing protection
Proof of Value:

1. Cloud Email Security
2. On-premise Email Security
3. Advance Phishing Protection
4. Cisco Threat Analyzer o365
Cisco Email Security – Zaštitite svoj najosjetljiviji dio sustava od napada