Audit & Penetration Test στο πλαίσιο του NIS2

Αντώνης Καλοχριστιανάκης, Sales Director
Ιωάννης Δασκαλόπουλος, Head of Security Services

WatchGuard

Digital Sima

sima security

Security Services

Βασικές Υπηρεσίες Ασφάλειας

sima security

- Penetration test
- Security Audit
- User Awareness
- ISMS / ISO 27001
- Risk Assessment

Ποιοι κάνουν Security Services

sima security

- Ανίχνευση κινδύνων και θωράκιση δικτύου.
- Κανονιστικό πλαίσιο κλάδου.
- Προϋπόθεση ανάληψης έργου
- Βελτίωση προφίλ / εξαγορά
- Προϋπόθεση συνεργασίας
- NIS 2
- Αφορά όλες τις εταιρείες

sima security

NIS 2

NIS2

Η Οδηγία NIS θεσπίζει βασικές απαιτήσεις και πρακτικές ασφάλειας για εταιρίες με παρουσία στην ΕΕ που είναι κρίσιμες

Έναρξη επιβολής
Οκτώβριος 2024

Εταιρείες που επηρεάζονται
160.000 vs 4.000

NIS2

Σε **σύγκριση** με το NIS1:

- Κάλυψη ενός πολύ ευρύτερου φάσματος βιομηχανιών και τομέων υπηρεσιών
- Αυστηρότερες ποινές επιβολής
- C-level πλέον λογοδοτεί
- Αυστηρότερη εποπτεία
- Αυστηρές διαδικασίες αναφοράς περιστατικών

NIS2 - ESSENTIAL vs IMPORTANT

sima security

Essential Entity Thresholds

?

250 EMPLOYEES + €50M ANNUAL TURNOVER

ESSENTIAL

IMPORTANT

Important Entity Thresholds

?

50 EMPLOYEES + €10M ANNUAL TURNOVER

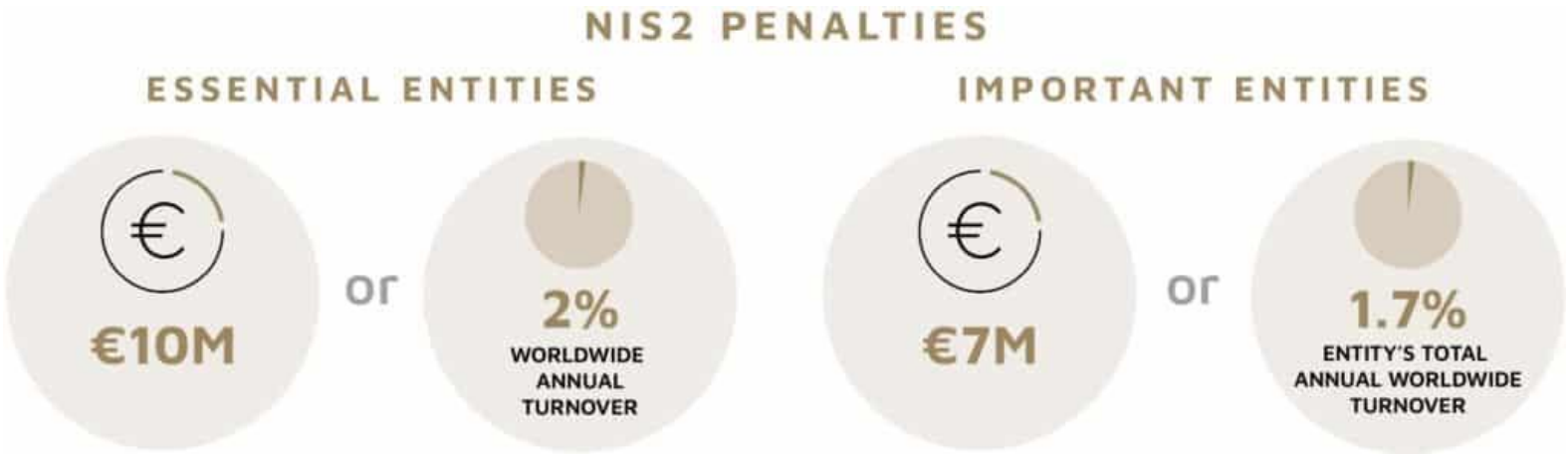
Τη γλύτωσαν....

NIS2 - ESSENTIAL vs IMPORTANT

Essential → Προληπτική παρακολούθηση συμμόρφωσης από τις ρυθμιστικές αρχές

Important → Έλεγχος συμμόρφωσης με το NIS2 σε περιστατικό ασφάλειας ή καταγγελία

Penalties →



NIS2

Ελάχιστες απαιτήσεις κανονισμού

- Risk analysis & Πολιτικές ασφαλείας
- Πολιτική διαχείρισης περιστατικών
- Business continuity
- Supply chain security
- Διαδικασία για διαχείριση Ευπαθειών
- Διαδικασίες για έλεγχο αποτελεσματικότητας του cyber risk management
- Cybersecurity training σε εργαζόμενους

NIS2

ISO 27001 → Το 80 έως 90% της συμμόρφωσης με το NIS2

Βήματα Προετοιμασίας →

1. Penetration test
2. Security Audit – GAP
3. ISMS

sima security

Penetration Test

Penetration Test

sima security

Έλεγχος κρίσιμων στοιχείων
(Firewall, Active Directory, Email Server, SQL Server και Web Server)

- ✓ Αυτοματοποιημένα εργαλεία.
- ✓ Προσπάθεια παρείσδυσης από εξειδικευμένη ομάδα τεχνικών.
- ✓ Έλεγχος για γνωστές αλλά και άγνωστες ευπάθειες όπως λάθη, παραλείψεις ή πρόβλημα στο σχεδιασμό.

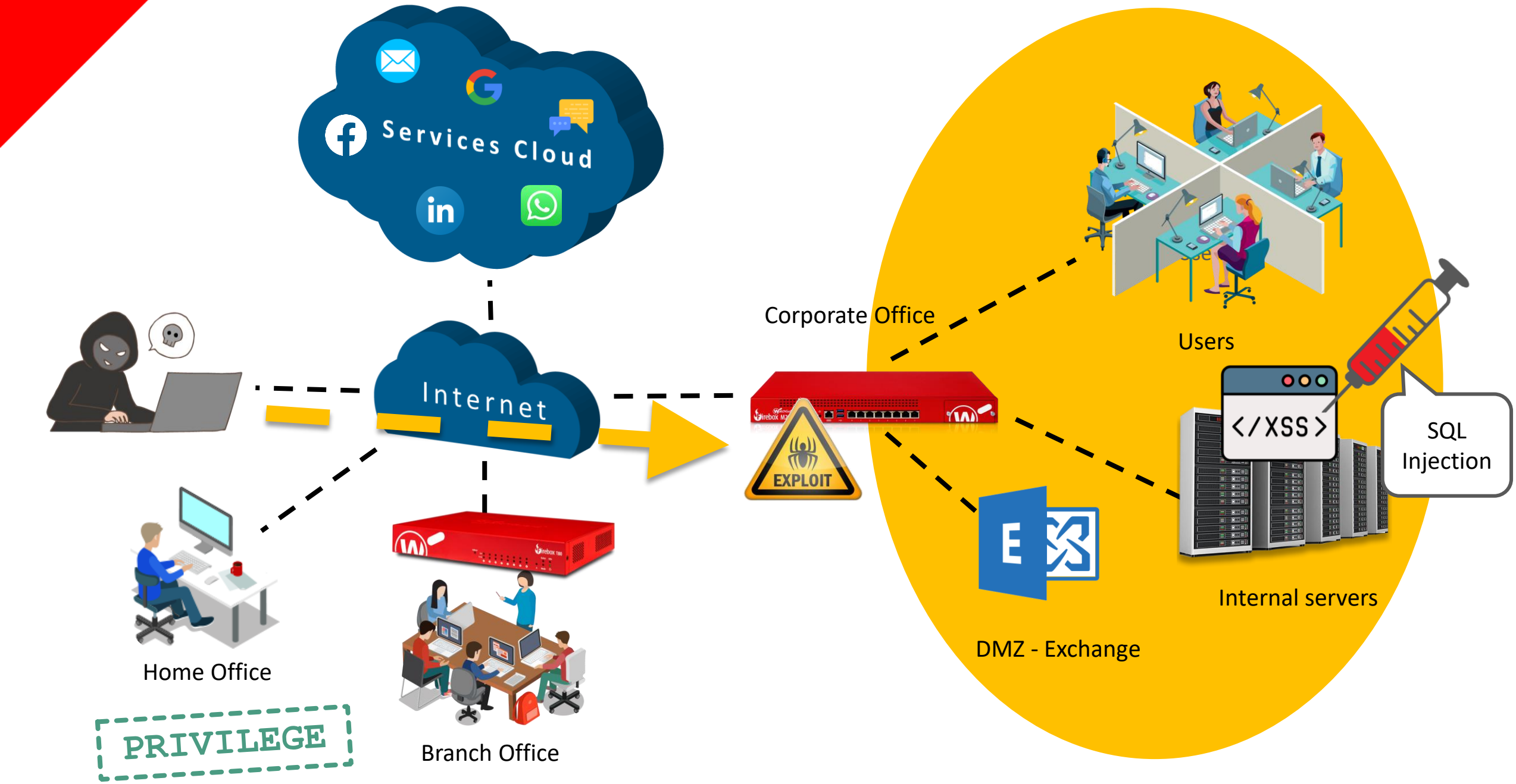
Αποτέλεσμα:

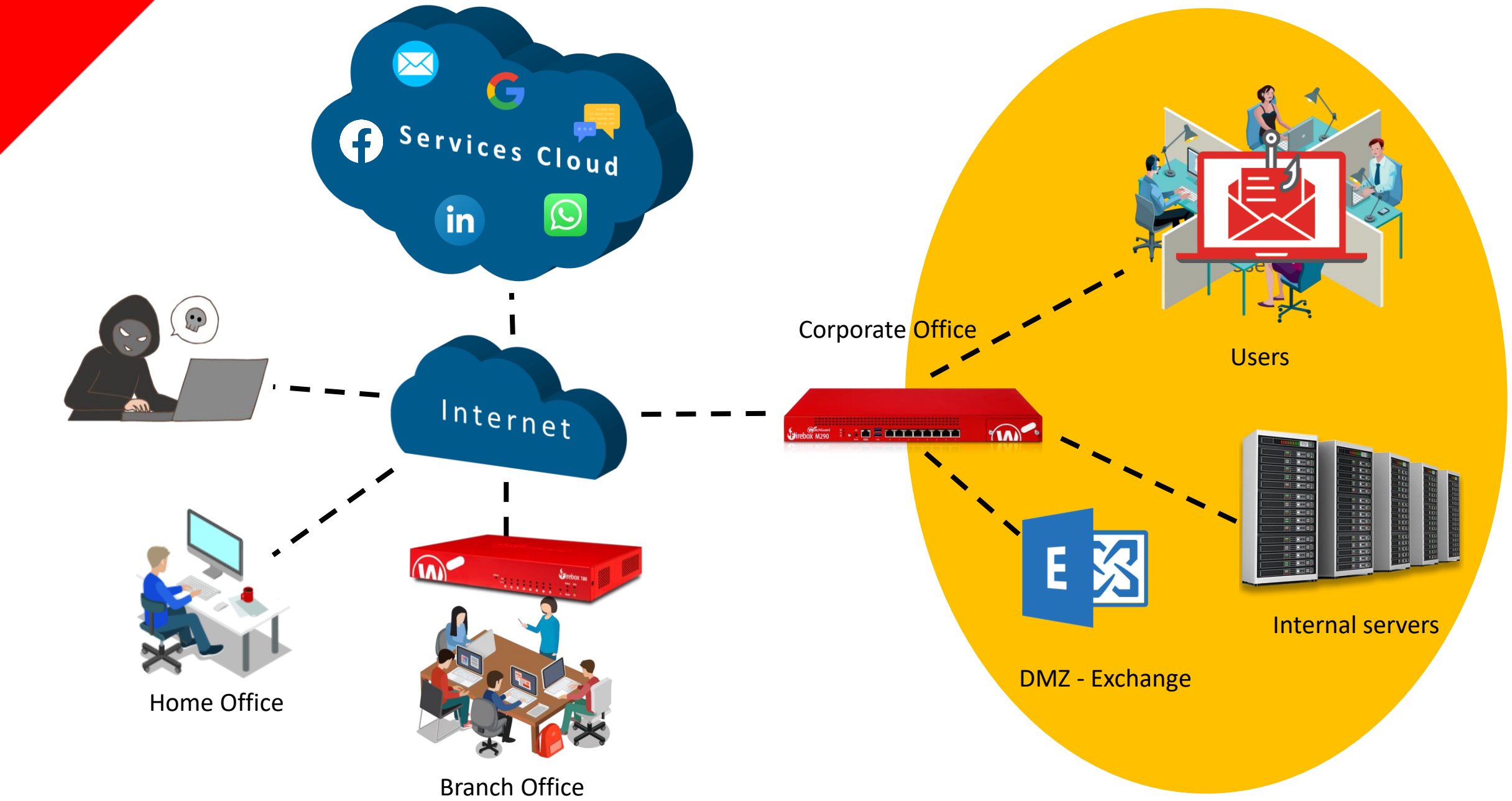
- Καταγραφή και αξιολόγηση των κινδύνων.
- Προτεινόμενες ενέργειες για την διόρθωσή τους.

Penetration Test

sima security

Ποιες είναι οι βασικές κατηγορίες Penetration Test;

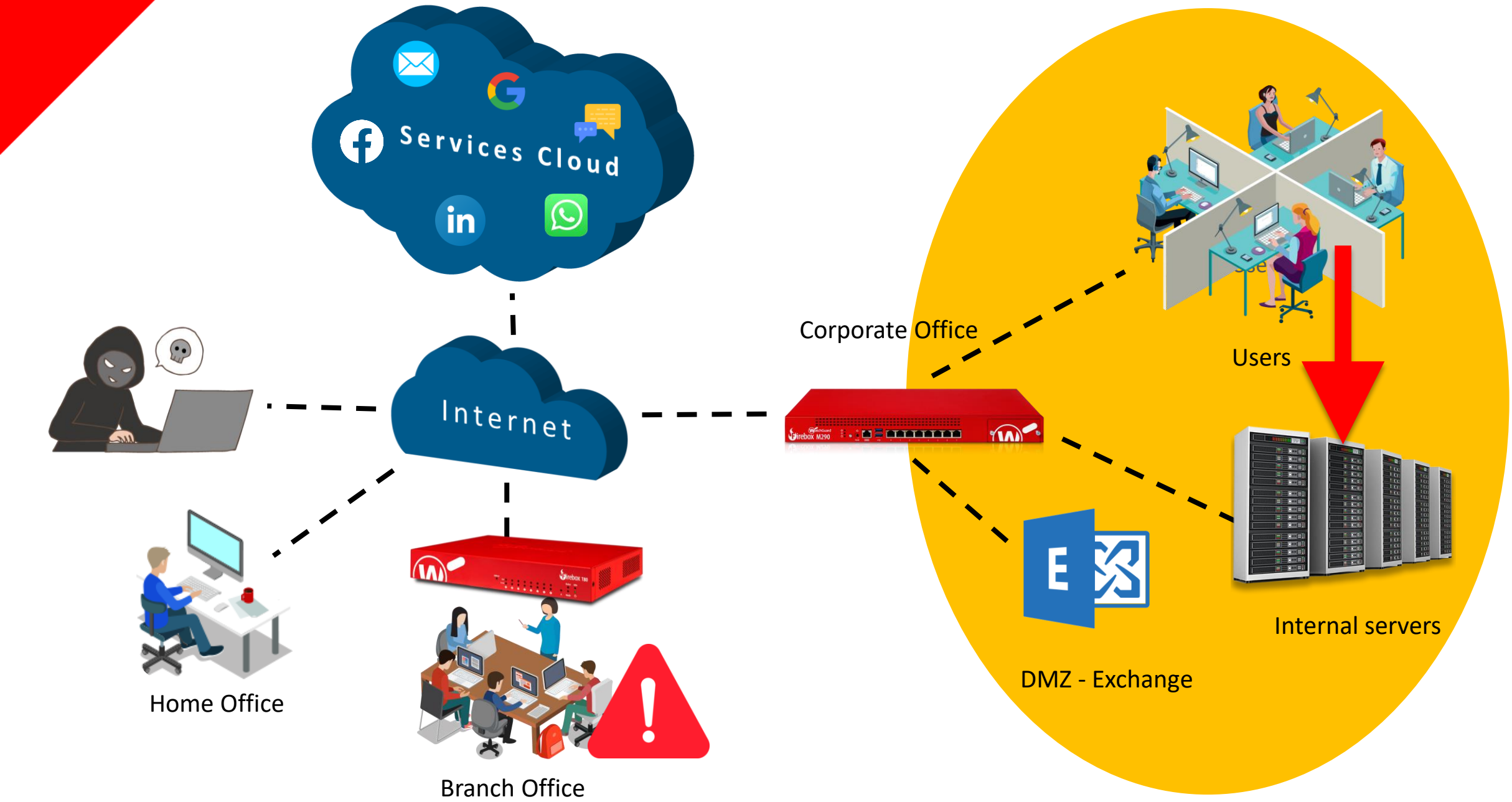

Services Cloud
Internet
Corporate Office
Users
EXPLOIT
</XSS>
SQL Injection
Internal servers
DMZ - Exchange
Home Office
Branch Office
PRIVILEGE


Services Cloud
Internet
Corporate Office
Users
Internal servers
DMZ - Exchange
Home Office
Branch Office

Penetration Test

sima security

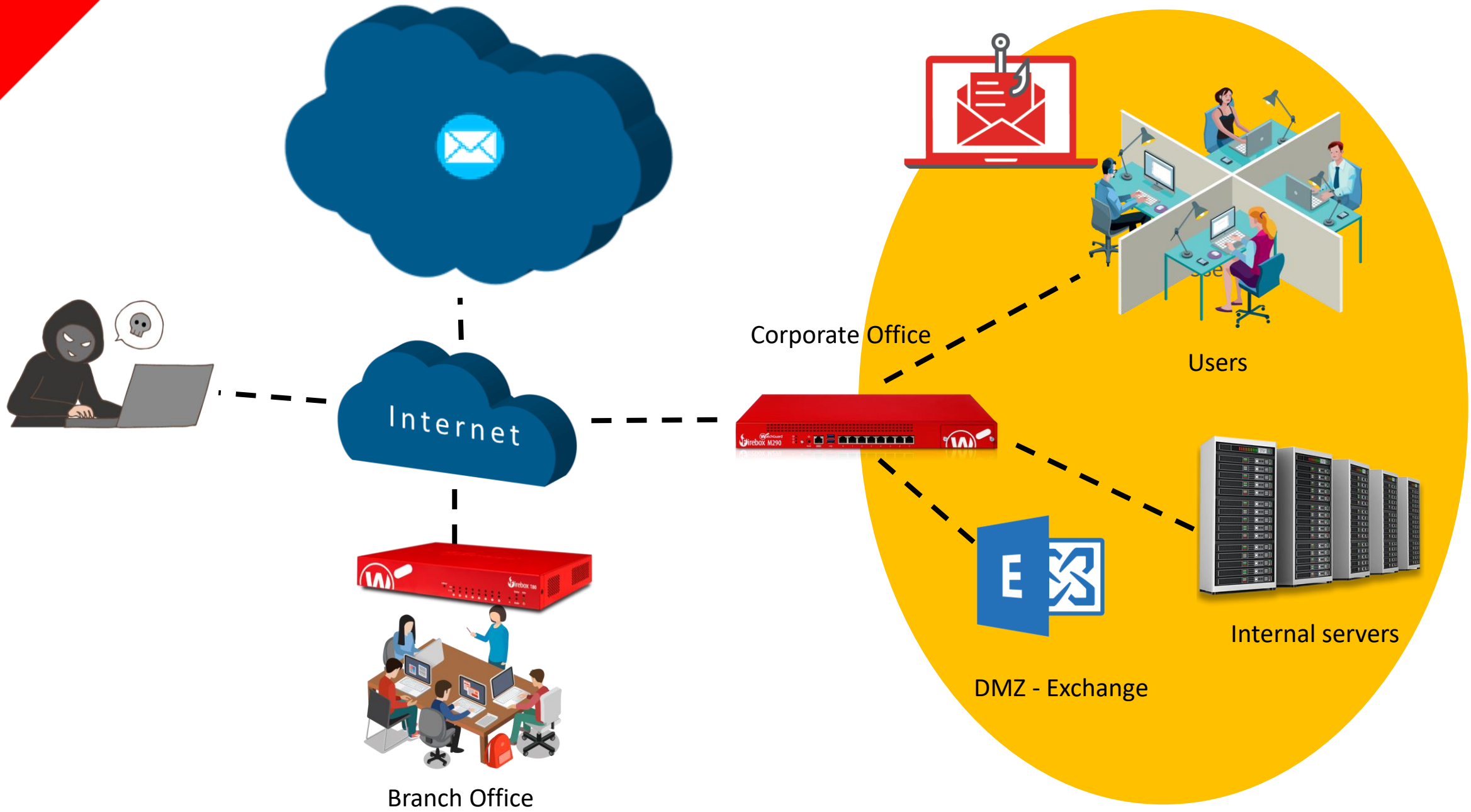
Υπάρχουν διαφοροποιήσεις σε ένα Internal Penetration Test; (σενάρια, δικαιώματα)


Services Cloud
Internet
Corporate Office
Users
Internal servers
DMZ - Exchange
Home Office
Branch Office

Penetration Test

sima security

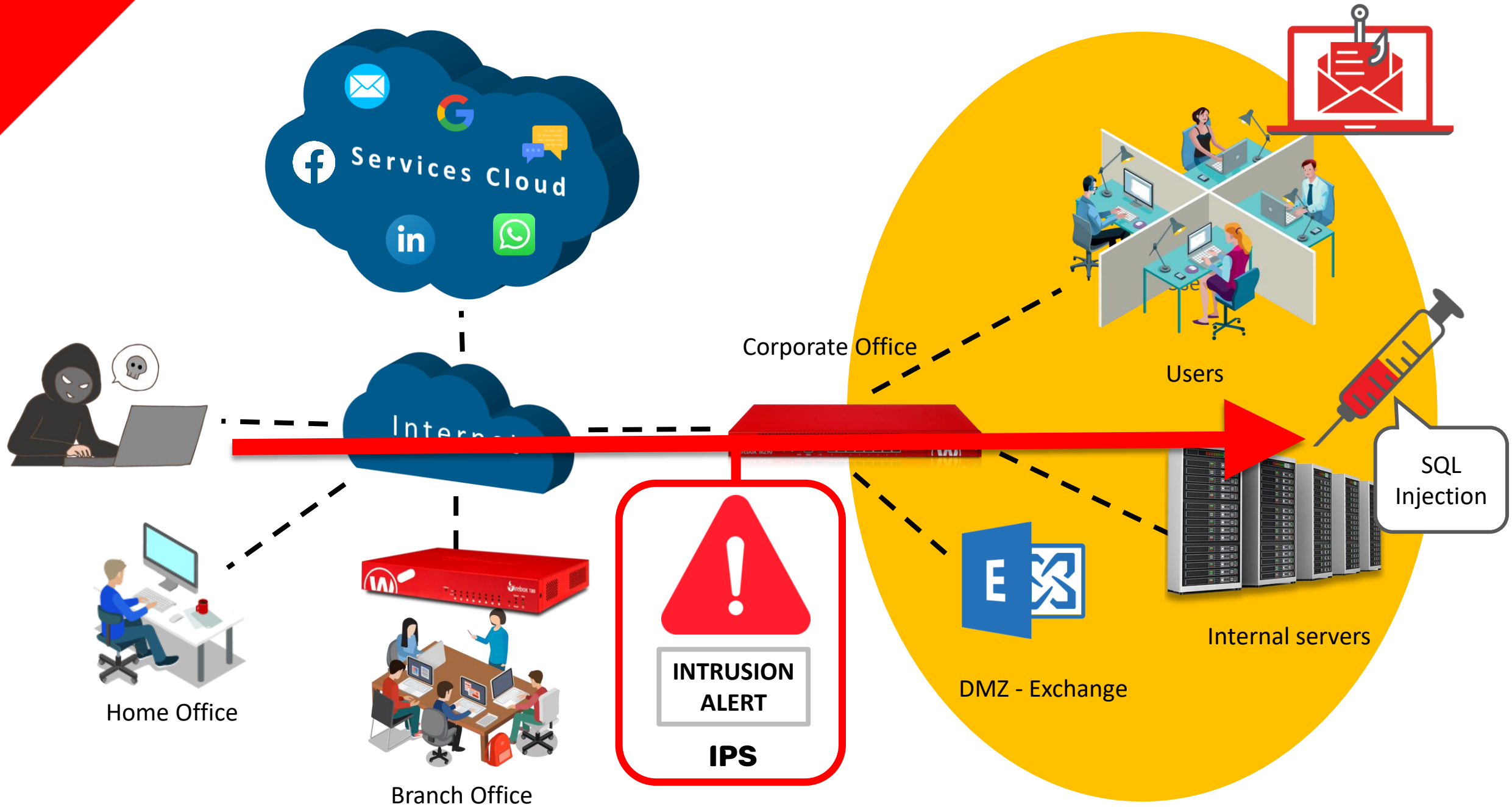
Πότε γίνεται Phishing simulation;


Internet
Corporate Office
Users
Internal servers
DMZ - Exchange
Branch Office

Penetration Test

sima security

Τι ευρήματα σχετίζονται με το NG Firewall;


Services Cloud
Internet
Corporate Office
Users
SQL Injection
Internal servers
DMZ - Exchange
INTRUSION ALERT
IPS
Home Office
Branch Office

Security Audit

sima security

Ποιες είναι οι βασικές κατηγορίες των Security Audit

IT Security Audit / Extended

sima security

Αποτελεσματικό εργαλείο για την **σφαιρική προστασία** των δικτύων.

- Ελέγχονται όλα τα στοιχεία του δικτύου.
- Διαπιστώνεται ο βαθμός συμμόρφωσης σε πρότυπα, κανόνες και πρακτικές.
- Καταγράφονται προβλήματα.

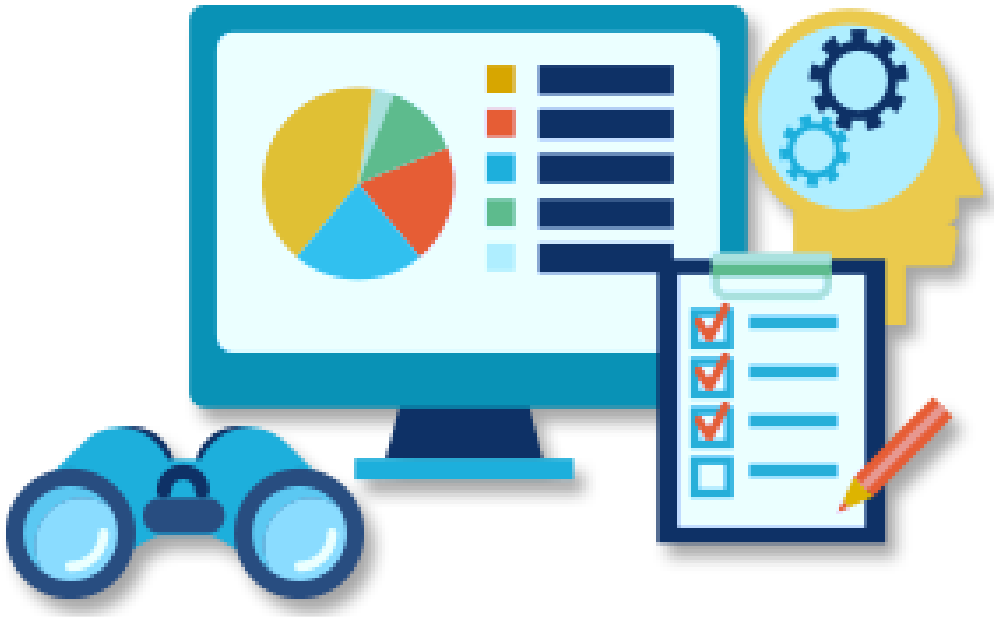
Το **Extended** βασίζεται στο **NIST** και επιπλέον ελέγχει διαδικασίες που μπορεί να γίνουν αντικείμενο εκμετάλλευσης.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

IT Security Audit / Extended

sima security

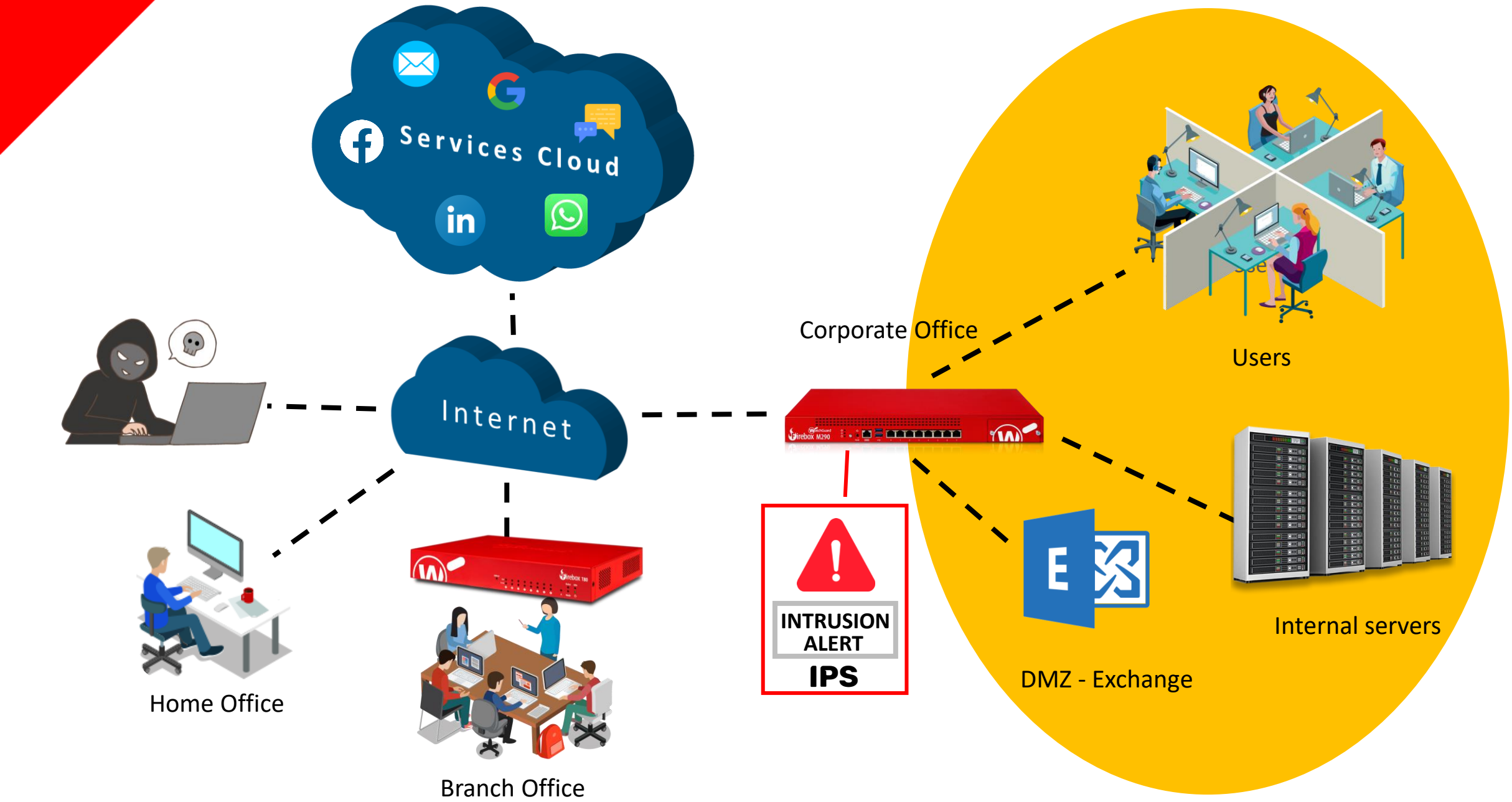
- Επισημαίνεται ο κίνδυνος που προκύπτει από κάθε πρόβλημα.
- Εκτιμάται το κόστος και οι πόροι που απαιτούνται για τη διόρθωση των προβλημάτων.
- Προτείνονται τρόποι βελτίωσης.



Security Audit

sima security

Ποια προβλήματα του NG Firewall αναδεικνύονται στο Audit και δεν τα βρίσκει το Penetration Test.


Services Cloud
Internet
Corporate Office
Users
Internal servers
DMZ - Exchange
INTRUSION ALERT
IPS
Home Office
Branch Office

Security Services

sima security

Είμαι IT/εξωτερικός συνεργάτης, πρέπει να με αγχώνει το report των Security Services

Security Services

sima security

- Υπάρχουν εξειδικεύσεις και μόνο ειδικοί μπορούν να βρουν και να αναδείξουν όλες τις πιθανές απειλές
- Χωρίς αποτελεσματικά ($/€) εργαλεία δεν γίνεται να γνωρίζουμε τις πλήρεις ευπάθειες ενός δικτύου.
- Είναι μοχλός πίεσης προς διοίκηση για να παρθούν τα σωστά αντίμετρα

Ευχαριστούμε!

WatchGuard

Digital Sima