COSMOS BUSINESS SYSTEMS AEBE

TURN Key SOLUTIONS

COSMOS BUSINESS SYSTEMS

SECURITY SOLUTIONS

Στρατηγικός Συνεργάτης σας για διαχείριση κυβερνοασφάλειας υποδομής Cyber Security Consulting, Services & Products

ΑΣΦΑΛΕΙΑ ΓΙΑ ΚΑΘΕ ΕΠΙΧΕΙΡΗΣΗ

Η Cosmos Business Systems, με πάνω από 30 χρόνια στην αγορά Πληροφορικής και χιλιάδες πελάτες, έχει ένα μοναδικό οικοσύστημα συνεργατών που υποστηρίζει τις ανάγκες πολλών χιλιάδων ευχαριστημένων πελατών και είναι και ενεργή στην προσφορά ολοκληρωμένων λύσεων ασφάλειας που καλύπτουν ένα ευρύ πεδίο και απευθύνονται σε μεγάλες, μεσαίες αλλά και μικρές επιχειρήσεις.

Με τρία υποκαταστήματα στην Αθήνα, Θεσσαλονίκη και Κύπρο, η Cosmos Business Systems προσφέρει και υπηρεσίες IT Consulting καθώς και ένα ολοκληρωμένο portfolio λύσεων ασφάλειας όπως και Security Audit, τεστ για ευπάθειες και τεστ διείσδυσης, σε συνδυασμό με ISO 9001 και ISO 27001 πιστοποιήσεις και χρόνια εμπειρίας στον τομέα υπηρεσιών πληροφορικής σε διαφόρους τομείς, όπως:

Συμμόρφωση με τον κανονισμό GDPR

Αναγνώριση και ανάλυση ευαίσθητων προσωπικών δεδομένων, GAP Analysis, DPIA report και υλοποίηση τεχνικών μέτρων που προκύπτουν από τον κανονισμό, όπως κρυπτογράφηση δεδομένων, αυθεντικοποίηση, κ.ά.

Συστήματα Ελέγχου Πρόσβασης και Αυθεντικοποίησης (NAC)

Συστήματα ελέγχου πρόσβασης ασφάλειας υπολογιστικών υποδομών και δικτύων.

Cloud και Data Center Security

Next Generation Firewalls για Data Centers, Database Protection.

Integrated Threat Detection and Defense

Endpoint Protection, E-mail Security, Sandboxing, Threat Intelligence

Securing Data and Applications

Data Loss Prevention, Endpoint Encryption, προστασία σημαντικών εφαρμογών από απειλές και βελτίωση της απόδοσης τους καθώς και load balancing.

Οι λύσεις ασφάλειας της Cosmos Business Systems περιλαμβάνουν:

- Network Firewalls.
- Λύσεις Cloud E-mail security.
- BYOD mobile device management λύσεις και λογισμικά.
- Λύσεις Endpoint security.
- Λύσεις Sandboxing για προστασία από στοχευμένες επιθέσεις (ATA's), και (APT's).
- Endpoint Encryption γνωστές λύσεις.
- Security Event Management (SIEM) γνωστές λύσεις.
- Υπηρεσίες ασφάλειας όπως Security Audit, Wireless Audit, Vulnerability Assessment (VA) και internal, external Penetration Testing.

Η ΑΥΞΑΝΟΜΕΝΗ ΑΝΑΓΚΗ ΓΙΑ ΑΣΦΑΛΕΙΑ

Η αύξηση στοχευμένων επιθέσεων και ransomware έχει καταστήσει πιο έντονα αναγκαία την διασφάλιση της ICT υποδομής από απειλές. Η αναμενόμενη εμφάνιση τεχνολογιών IoT, έχει από μόνη της γίνει ένας σημαντικός παράγοντας που χρήζει λύσεις ασφάλειας. Επιπρόσθετα, ο κανονισμός GDPR είναι για κάθε εταιρεία υποχρεωτική προτεραιότητα που γεννάει ανάγκες για κρυπτογράφηση δεδομένων, αυθεντικοποίηση χρηστών, data loss prevention και endpoint protection τεχνολογίες.

Οι τάσεις στην κυβερνοασφάλεια συγκεντρώνονται γύρω από:

- Artificial Intelligence (AI) επιθέσεις και Machine Learning τεχνικές.
- Κυβερνοπόλεμο ανάμεσα σε χώρες που είναι πια συχνό φαινόμενο.
- Αύξηση των επιθέσεων ransomware.
- Πρόστιμα για μη συμμόρφωση με τον κανονισμό GDPR.
- Ασφαλιστικές εταιρείες που προσφέρουν κυβερνοασφάλιση.
- Αύξηση στο crypto mining hijacking υπολογιστικής ισχύος σε υπολογιστές με την μορφή bitcoins ή άλλων cryptocurrency.
- Γενική έλλειψη ασφάλειας σε IoT συσκευές.

Όλα αυτά συμβαίνουν ενώ το παράνομο crimeware στον τομέα της ασφάλειας αυξάνει ως μία ενεργή και κερδοφόρα επιχείρηση.

ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΥΜΒΑΙΝΟΥΝ ΣΕ ΟΛΑ ΤΑ ΕΙΔΗ ΕΤΑΙΡΕΙΩΝ

Μερικές από τις μεγαλύτερες επιθέσεις έγιναν σε πολύ γνωστές εταιρείες, υποδηλώνοντας ότι κανείς δεν είναι ασφαλής.

Κοινωνικά Δίκτυα
Facebook (87 εκατομμύρια user profiles).
Twitter (330 εκατομμύρια passwords χρηστών).
Yahoo (2017) (3 δισεκατομμύρια δεδομένα συνδρομητών).

Ο Τομέας της Υγείας και των Ασφαλιστικών Εταιρειών είχε παραβιάσεις ασφάλειας που οδήγησαν στην κλοπή αρχείων δεδομένων ασθενών, διευθύνσεων, ονομάτων και ιατρικών αρχείων. Τα δεδομένα υγείας έχουν δεκαπλάσια αξία για τους hackers από ότι οι τραπεζικοί λογαριασμοί, καθώς παραμένουν αναλλοίωτα με το χρόνο.

Τομέας Υγείας
Health South East, Νορβηγία Norway, 2.9 εκατομμύρια ιατρικά αρχεία.
Under Armour, 150 εκατομμύρια ιατρικά δεδομένα συνδρομητών της εφαρμογής MyFitnessPal.

Τηλεπικοινωνιακοί Πάροχοι
DU Caller China, 2 δισεκατομμύρια δεδομένα συνδρομητών.
RiverCity Media 2017, 1.3 δισεκατομμύρια δεδομένα συνδρομητών.

Επιχειρήσεις με ευαίσθητα δεδομένα
Vtech Toys, 6.4 εκατομμύρια ονόματα, διευθύνσεις, φωτογραφίες παιδιών.

Aetna Ασφαλιστική, 12,000 ιατρικοί φάκελοι ασθενών HIV με ονόματα και διευθύνσεις.

Τομέας Λιανικής Πώλησης
Μερικές από τις μεγαλύτερες παραβιάσεις ασφάλειας έγιναν σε μεγάλες και γνωστές επιχειρήσεις λιανικής πώλησης όπως:

- **eBay**, 145 εκατομμύρια passwords, emails, usernames και διευθύνσεις.
- **Target**, 40 εκατομμύρια δεδομένα πιστωτικών καρτών.
- **Saks Fifth Avenue**, 5 εκατομμύρια δεδομένα πιστωτικών καρτών.

Και η λίστα συνεχίζεται με τα **Sears**, **Delta**, **Best Buy, Solarwinds** και άλλα.
Μία από τις μεγαλύτερες παραβιάσεις ασφαλείας ήταν αυτή της **Equifax**, ενός πρακτορείου πιστοληπτικής ικανότητας όπου εκλάπησαν προσωπικά στοιχεία πληρωμών, δανείων και λογαριασμών από 143 εκατομμύρια Αμερικανούς.

ΤΑ ΔΙΚΤΥΑ IT ΕΙΝΑΙ ΑΝΟΙΧΤΑ ΣΕ ΕΠΙΘΕΣΕΙΣ

Η πολυπλοκότητα των IT δικτύων σήμερα με τις πολλές διαφορετικές τεχνολογίες, έχει αλλάξει την παραδοσιακή δομή τους. Τα δίκτυα σήμερα συμπεριλαμβάνουν λύσεις από διάφορους κατασκευαστές με διαφορετικά λειτουργικά συστήματα. Για τις επιχειρήσεις οι αλλαγές αυτές είναι θετικές, επιτρέποντας τους να αναπτυχθούν και να εκμεταλλευτούν τις νέες επιχειρηματικές ευκαιρίες. Αλλά από πλευράς ασφάλειας, η εισαγωγή νέων τεχνολογιών και η τάση BYOD άνοιξαν πολλαπλούς νέους τρόπους για διείσδυση στο δίκτυο τους.

Οι στρατηγικές ασφαλείας έχουν επίσης εξελιχθεί για να αντιμετωπίζουν τις ευπάθειες που προκύπτουν από το Internet, το Cloud, το IoT, τα ασύρματα δίκτυα και την συνεχή ανάδυση νέων τύπων απειλών όπως τα ransomware. Τα παραπάνω σε συνδυασμό με το γεγονός ότι τα περισσότερα δίκτυα έχουν επίπεδη αρχιτεκτονική μέσα από την εξωτερική περίμετρο, κάνουν πιο εύκολη την μετάδοση των απειλών μέσα στο δίκτυο μετά από μία παραβίαση ασφάλειας.

Εξαιτίας αυτού, η δικτυακή χωροθέτηση έχει καταστεί απαραίτητη για την προστασία ζωτικών πληροφοριών και εφαρμογών που χρειάζονται προστασία πίσω από ισχυρές λύσεις ασφάλειας. Οι τεχνικές sandboxing είναι τώρα περισσότερο από ποτέ αναγκαίες για να σταματήσουν άγνωστες απειλές που τα antivirus δεν μπορούν να πιάσουν, από το να εισέλθουν στο δίκτυο.

Επιπρόσθετα, η απόσπαση σημαντικών δεδομένων έχει γίνει ευκολότερη επίσης. Το Shadow IT, ή χρήση μη εξουσιοδοτημένων εφαρμογών όπως Hightail και Dropbox, επίσης υποδεικνύει τους πολλαπλούς τρόπους που μπορούν να διαφύγουν δεδομένα από ένα δίκτυο. Σημεία εισαγωγής και εξαγωγής μέσα και έξω από δίκτυα μπορεί να είναι κάμερες, USB's, BYOD όπως κινητά τηλέφωνα, tablet και laptop, ασύρματα δίκτυα, wearables, IoT συσκευές, ηλεκτρονικοί συναγερμοί και άλλα. Η έλευση όλο και περισσότερων έξυπνων συσκευών και οικιακών στην αγορά που έχουν διεύθυνση IP και μπορούν να συνδεθούν με το οικιακό δίκτυο, προμηνύει νέους τρόπους διείσδυσης απειλών μέσω IoT.

Η ΑΝΑΓΚΗ ΓΙΑ ΑΣΦΑΛΗ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Ένα ασύρματο δίκτυο μπορεί να παραβιαστεί μέσα σε λίγα λεπτά, χρησιμοποιώντας συγκεκριμένες τεχνικές hacking. Τα ασύρματα δίκτυα ήταν πάντοτε ευάλωτα σε επιθέσεις, αλλά σήμερα περισσότερο από ποτέ είναι πλέον εύκολο να εισέλθει κάποιος μέσα στο δίκτυο μιας εταιρείας μέσω pineapple και rogue access points. Σκεφτείτε πότε ήταν η τελευταία φορά που ελέγχθηκε το ασύρματο δίκτυο για rogue access points και έγινε ένα wireless audit. Πέρυσι περίπου 10 διαφορετικές ευπάθειες εντοπίστηκαν στο πρωτόκολλο ασύρματης πρόσβασης WPA και WPA2 υπεύθυνο για την ασφάλεια ασύρματων δικτύων. Η απειλή KRACK Wi-Fi χρησιμοποιεί αυτές τις ευπάθειες για να υποκλέψει κλειδιά στην επικοινωνία των access points και αποκρυπτογραφεί πακέτα δεδομένων, στέλνοντας malware μέσα στη ροή τους και υποκλέπτοντας ασφαλείς ασύρματες συνδέσεις.

Η ασύρματη παραβίαση ασφάλειας Krack Wi-Fi έχει επηρεάσει εκατομμύρια συσκευών, υποκλέπτοντας αριθμούς πιστωτικών καρτών, passwords, μηνύματα chat, emails και φωτογραφίες. Η κρυπτογράφηση δεδομένων σε επίπεδο τερματικών συσκευών (λύσεις MDM/MAM) και η ελεγχόμενη πρόσβαση στα ασύρματα δίκτυα (λύσεις NAC) καθώς και η αυθεντικοποίηση των χρηστών για να είσοδο σε κινητά και εφαρμογές, είναι όλοι καλοί τρόποι να ασφαλιστούν τα ασύρματα δίκτυα.

Επιπλέον τεχνικό μέτρο είναι και το **Vulnerability Assessment** (VA) με τον εσωτερικό έλεγχο υποδομής για ύπαρξη ευπαθειών (CVEs).

Network Access Control (NAC)

Συστήματα ελέγχου πρόσβασης καλύπτουν ανάγκες ελέγχου των συσκευών του χρήστη (endpoint devices) που συνδέονται στο εταιρικό δίκτυο, με σκοπό την μείωση των απειλών από αυτά προς το υπόλοιπο εταιρικό δίκτυο.

Τυχόν ανεξέλεγκτη σύνδεση τους (π.χ. φορητοί υπολογιστές), είτε του προσωπικού είτε εξωτερικών συνεργατών, στο εταιρικό δίκτυο είναι μια από τις μεγαλύτερες απειλές για την ασφάλεια καθώς εκτός

του εταιρικού δικτύου συνδέονται και σε άλλα μη ελεγχόμενα δίκτυα.

Έτσι τα παραπάνω απαιτούν ένα ολοκληρωμένο σύστημα ελέγχου πρόσβασης στο δίκτυο που θα ελέγχει κεντρικά κάθε συσκευή που θα προσπαθεί να συνδεθεί.

Ακολουθούν ενδεικτικοί έλεγχοι που πραγματοποιούνται στα συστήματα που ζητούν πρόσβαση στο δίκτυο:

- Κατάλληλη έκδοση λειτουργικού συστήματος (π.χ. μόνο Windows 10 επιτρέπεται να συνδέονται).
- Αν έχει εγκαταστημένα τα κατάλληλα security ή άλλα critical patches.
- Αν έχει ενημερωμένο πρόσφατα Antivirus λογισμικό (γενικά ή/και συγκεκριμένου vendor π.χ. Symantec/ ESET).
- Αν έχει DLP λογισμικό.
- Αν εκτελείται ως Virtual Machine (VM).
- Επιτυχή αναγνώριση και εξουσιοδότηση του τερματικού αλλά και του χρήστη.
- Επιτυχή έλεγχο του τερματικού σε επίπεδο πολιτικής ασφάλειας (π.χ. τρέχει Antimalware,personal firewall, κτλ.).
- Να διαθέτει προστασία (DLP) για αποφυγή διαρροής πληροφοριών.
- Αν είναι συσκευή Voice Over IP.

Η Cosmos Business Systems είναι σε συνεργασία με εξειδικευμένους κατασκευαστές λύσεων ελέγχου πρόσβασης, όπως τους Aruba ClearPass, FortiNAC, Cisco NAC.

ΠΡΟΣΤΑΣΙΑ SPEAR PHISHING E-MAIL (on premise και στο cloud)

Αναλύοντας με περισσότερη λεπτομέρεια τους τρόπους προστασίας του δικτύου, τα συνημμένα σε e-mail όπως και τα links που περιέχονται μέσα σε αυτά, είναι από τους πιο κοινούς τρόπους παραβίασης ασφάλειας.

Τα e-mail είναι δημοφιλή μέσα εξάπλωσης spam, malware και phishing επιθέσεων, χρησιμοποιώντας τεχνικές εξαπάτησης για να δελεάσουν τους παραλήπτες να δώσουν ευαίσθητες πληροφορίες, να ανοίξουν συνημμένα αρχεία ή να συνδεθούν πάνω σε hyperlinks τα οποία εγκαθιστούν malware στην συσκευή του θύματος. Το e-mail είναι επίσης ένα σύνηθες μέσο εισόδου για χάκερς που επιδιώκουν να αποκτήσουν πρόσβαση σε επιχειρηματικά δίκτυα και να αποσπάσουν σημαντικά σε απολαβές εταιρικά δεδομένα. Η ασφάλεια του Email είναι λοιπόν αναγκαία και για το άτομο αλλά και για την επιχείρηση. Τα Phishing emails στοχεύουν στο να αποσπάσουν πληροφορίες ρωτώντας τυπικά παραλήπτες να επιβεβαιώσουν τα passwords τους, τους αριθμούς κοινωνικής ασφάλισης, τους τραπεζικούς λογαριασμούς τους και τις πιστωτικές τους κάρτες, πολλές φορές στέλνοντας τους σε πλαστές ιστοσελίδες τραπεζών που μοιάζουν ακριβώς όπως τις πραγματικές

ώστε να εξαπατήσουν τα θύματα τους στο να εισάγουν τους λογαριασμούς τους ή τα οικονομικά τους στοιχεία. Η κρυπτογράφηση των email, οι σουίτες προστασίας ηλεκτρονικής αλληλογραφίας, η επικύρωση τους και τα σεμινάρια ασφάλειας των εργαζομένων, είναι οι καλύτερες πρακτικές ασφάλειας που εφαρμόζονται για να διασφαλίσουν την ηλεκτρονική αλληλογραφία οργανισμών.

Η Cosmos Business Systems είναι σε συνεργασία με εξειδικευμένους κατασκευαστές λύσεων ασφάλειας ηλεκτρονικής αλληλογραφίας.

ΠΡΟΣΤΑΣΙΑ ENDPOINT

Οποιαδήποτε συσκευή smartphone, tablet, laptop ή USB stick αποτελεί σημείο εισόδου απειλών. Οι λύσεις endpoint security στοχεύουν στο να διασφαλίσουν επαρκώς κάθε τερματική συσκευή που συνδέεται στο δίκτυο και να μπλοκάρουν προσπάθειες πρόσβασης και άλλη διακινδυνευμένη δραστηριότητα σε αυτά τα τερματικά εισόδου. Καθώς περισσότερες επιχειρήσεις υιοθετούν πρακτικές BYOD (Bring Your Own Device) από απομακρυσμένους εργαζόμενους, η περίμετρος ασφάλειας του επιχειρηματικού δικτύου βρίσκεται σε κίνδυνο παραβίασης. Η ανάγκη για αποτελεσματική ασφάλεια στα τερματικά έχει αυξηθεί σημαντικά, εν όψει της αύξησης στις απειλές κινητών συσκευών και της εξάρτησης των εργαζομένων από αυτές, καθώς και της χρήσης οικιακών υπολογιστών και laptop για σύνδεση στα δίκτυα εταιρειών. Διαφοροποιώντας το endpoint security από τα λογισμικά antivirus, εν μέσω του endpoint security framework, τα endpoints χρήζουν ασφάλειας ατομικά. Οι λύσεις endpoint security πρέπει να έχουν λειτουργικότητα για data loss prevention, insider threat protection, disk, endpoint και email encryption, έλεγχο πρόσβασης σε εφαρμογές και δίκτυα, data classification, ανίχνευση τερματικών και απάντηση καθώς και privileged access management. Η Cosmos Business Systems έχει εμπειρία και προσφέρει ολοκληρωμένες λύσεις endpoint security σε συνεργασία με τις καλύτερες κατασκευάστριες εταιρείες λύσεων endpoint security.

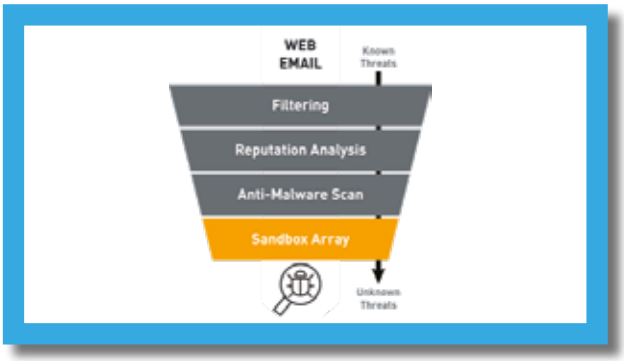
ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΩΝ ΑΓΝΩΣΤΩΝ ΑΠΕΙΛΩΝ (sandboxing)

Οι στοχευμένες επιθέσεις, πολύ συχνά αναφερόμενες ως APTs ή Advanced Persistent Threats, διεισδύουν τους υφιστάμενους ελέγχους ασφάλειας προκαλώντας σημαντικές απώλειες στις επιχειρήσεις. Οι επιχειρήσεις από τη μεριά τους προσπαθούν να εστιάσουν στη μείωση των ευπαθειών και στην αύξηση παρακολούθησης για την αποφυγή στοχευμένων επιθέσεων.

Οι τεχνικές sandboxing επιτρέπουν την ανάλυση των συνημμένων σε email και internet links ώστε να ανακαλύψουν απειλές για τις οποίες δεν υπάρχουν ακόμα signatures σε προγράμματα antivirus, ή δεν είναι γνωστές.

Οι περισσότερες από αυτές τις στοχευμένες επιθέσεις έρχονται με την μορφή ransomware (π.χ. Cryptolocker, WannaCry, Petya malware) και επεκτείνονται μέσω συνημμένων σε email. Για αυτό τα sandbox σε εικονικό λογισμικό ή φυσική μηχανή ή στο cloud βοηθούν τις επιχειρήσεις να ανιχνεύσουν και να απομονώσουν αυτές τις επιθέσεις πριν επεκταθούν στο δίκτυο.

Η CBS προσφέρει τις καλύτερες sandboxing τεχνολογίες για την προστασία από ATA's ή advanced targeted attacks και persistent threats, που σχεδιάζουν να μπουν στην επιχείρηση σας σε συνεργασία με πληθώρα κατασκευαστών και εμπειρία στον χώρο.



ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟ GDPR

Ο υφιστάμενος κανονισμός προστασίας προσωπικών δεδομένων της Ευρωπαϊκής Ένωσης (GDPR, σε ισχύ από 25 Μαΐου του 2018), απαιτεί λειτουργικές αλλαγές σε οργανισμούς σύμφωνα με το Data Protection Directive 95/46/EC και όλες οι εταιρείες χρειάζονται να συμμορφωθούν, καθώς ο κανονισμός αφορά όλες τις εταιρείες που διαχειρίζονται προσωπικά δεδομένα Ευρωπαίων πολιτών. Οι εταιρείες πρέπει να δίνουν το δικαίωμα στην πρόσβαση και στη λήθη για τα προσωπικά δεδομένα και μπορεί (σε περίπτωση διαρροής από αμέλεια τους) να έχουν πρόστιμο μέχρι και 20 εκατομμύρια ευρώ ή 4% του συνολικού τους τζίρου.

Η Cosmos Business Systems έχει πραγματοποιήσει παραπάνω από 40 έργα συμμόρφωσης με το GDPR σε διάφορες επιχειρήσεις και συνεχίζει με την τεχνική φάση δύο των απαιτήσεων για την συμμόρφωση, με έργα κρυπτογράφησης, επικύρωσης και DLP. Επίσης διαθέτει Data Protection Officer (DPO) με αρκετά χρόνια εμπειρίας στο Security Compliance. Η εταιρεία έχει πιστοποιήσεις ISO9001, ISO22301, ISO2000 και ISO27001 και δύναται να κάνει σχετικά έργα.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ

Η κρυπτογράφηση δεδομένων είναι απαίτηση του κανονισμού GDPR και περιλαμβάνει κρυπτογράφηση των τριών φάσεων δεδομένων, δηλαδή Data at Rest, Data in Motion και Data in Use. Αφορά βάσεις δεδομένων και κρυπτογράφηση σε δίσκους, email, κινητά και τερματικές συσκευές. Η Cosmos Business Systems συνεργάζεται με vendors με ολοκληρωμένες λύσεις για Disk Encryption, Endpoint Encryption, Server Encryption, Email Encryption και Database Encryption.

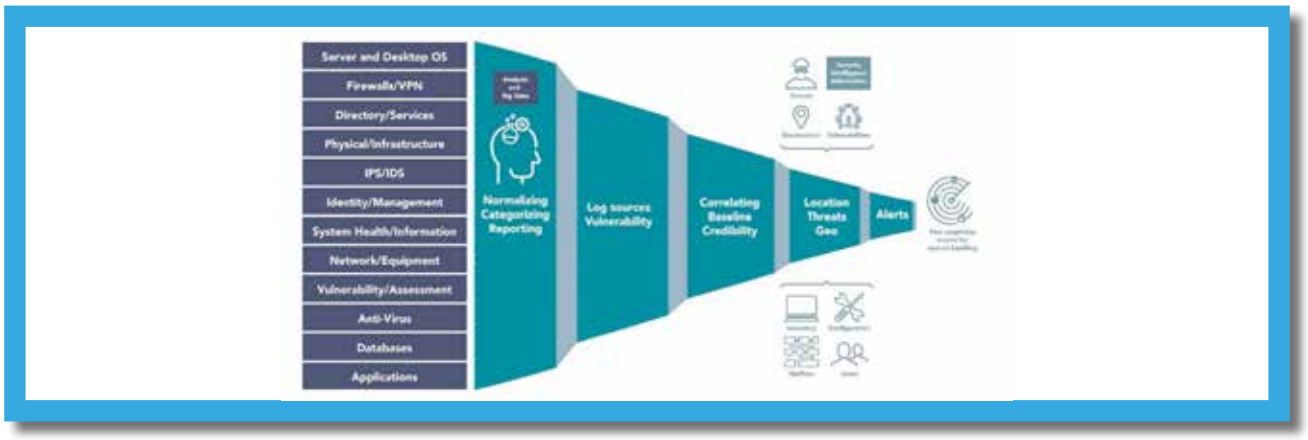
Η Gartner συνιστά ένα checklist για εργαλεία κρυπτογράφησης για επιχειρήσεις που περιλαμβάνει λύσεις με παρόμοιες πολιτικές κρυπτογράφησης σε όλες τις συσκευές, έτσι ώστε η διαχείριση να έχει συνοχή όχι

μόνο για Windows και OS X συστήματα, αλλά και για μικρότερες κινητές συσκευές. Επίσης προτείνει οι λύσεις να έχουν μία κονσόλα διαχείρισης για τις πολιτικές που ακολουθούνται σε όλες τις συσκευές και χαρακτηριστικά backup, έτσι ώστε όταν οι συσκευές δεν είναι διαθέσιμες να είναι δυνατόν να αποσαφηνιστεί ποια δεδομένα έχουν χαθεί – και να ανακτώνται αυτά τα δεδομένα.

Η Cosmos προσφέρει λύσεις bundle μαζί με Data Loss Prevention, καλύπτοντας έτσι τις απαιτήσεις της Φάσης Δύο του GDPR Phase 2 που αφορούν τεχνικές απαιτήσεις.

ΛΥΣΕΙΣ SIEM

Προτείνουμε λύση συστήματος κεντρικής διαχείρισης (συλλογή και αποθήκευση) συμβάντων Ασφάλειας (κ όχι μόνο) για την παροχή μιας λύσης διαχείρισης ασφάλειας η οποία θα εξελίσσεται και θα επεκτείνεται καλύπτοντας μελλοντικές ανάγκες. Συνδυάζει δυνατότητες *log management*, correlation, *threat detection* και *compliance management* σε μια ενιαία ολοκληρωμένη λύση ασφάλειας που θα αξιοποιεί logs/events/traps/flows κ.λπ., ταχύτατα και από το σύνολο της υποδομής. Έτσι πολλαπλασιάζεται η δυνατότητα παρακολούθησης της δικτυακής δραστηριότητας, των ενεργειών των χρηστών και της συμπεριφοράς των εφαρμογών, προσφέροντας ολοκληρωμένη εικόνα σχετικά τις πιθανές απειλές μέσα στην IT υποδομή. Παρακάτω απεικονίζεται γραφικά η διαδικασία εισόδου ΚΑΘΕ είδους μηνύματος και η σταδιακή αξιολόγηση τους σε κάθε στάδιο, για την σχετική κατάληξη σε κάποιο πραγματικό συμβάν.



DATA LOSS PREVENTION

Σε κάθε εταιρικό δίκτυο διακινούνται, αποθηκεύονται και επεξεργάζονται μια σειρά από ευαίσθητα δεδομένα, η προστασία της εμπιστευτικότητας και ακεραιότητας των οποίων αποτελεί κύριο μέλημα. Πιθανή μη εξουσιοδοτημένη πρόσβαση, κακόβουλη χρήση ή διαρροή των δεδομένων αυτών από χρήστες της υποδομής θα εκθέσει ανεπανόρθωτα την αξιοπιστία της εταιρίας σε επίπεδο επιχειρησιακής λειτουργίας με σοβαρές κοινωνικές και οικονομικές συνέπειες.

Παρόλο που κάθε εταιρικό δίκτυο περιλαμβάνει μια σειρά από προηγμένους τεχνολογικούς μηχανισμούς όπως π.χ. Firewalls, IPS, content security, strong authentication, access management κ.α., οι οποίοι θωρακίζουν σε σημαντικό βαθμό την επιχειρηματική λειτουργία της υποδομής είναι γεγονός ότι οι μηχανισμοί αυτοί επικεντρώνονται κατά κύριο λόγο **στον έλεγχο της πρόσβασης** στα κρίσιμα συστήματα και τα δεδομένα αυτών και την προστασία τους από προσπάθειες μη εξουσιοδοτημένης πρόσβασης. Αυτό είναι μεν βασικό και απαραίτητο, θεωρείται όμως ανεπαρκές για την ολοκληρωμένη προστασία των ευαίσθητων δεδομένων.

Βασική αδυναμία των μηχανισμών αυτών είναι η έλλειψη του απαιτούμενου ελέγχου και καταγραφής **της χρήσης** των δεδομένων αυτών από τους **εξουσιοδοτημένους χρήστες** της υποδομής. Η παντελής έλλειψη ελέγχου και παρακολούθησης των ενεργειών που πραγματοποιούν οι εξουσιοδοτημένοι χρήστες, συμπεριλαμβανομένων

και των διαχειριστών, στα κρίσιμα δεδομένα της υποδομής δημιουργεί ένα τεράστιο κενό ως προς την ασφάλεια των δεδομένων αυτών.

Για την αποτελεσματική προστασία των κρίσιμων δεδομένων της υποδομής απαιτείται η προμήθεια και υλοποίηση μιας ολοκληρωμένης λύσης προστασίας δεδομένων από διαρροή (DLP). Το εν λόγω σύστημα θα πρέπει να διασφαλίζει την προστασία και παρακολούθηση της ροής των κρίσιμων δεδομένων μέσα και έξω από το «κλειστό» δίκτυο παραγωγής. Οπουδήποτε μπορεί να βρίσκονται αυτά τα δεδομένα λ.χ. σταθμοί εργασίας, Servers, μέσα ή έξω από τον οργανισμό, το σύστημα θα πρέπει να βρίσκεται εκεί για να παρακολουθεί, καταγράφει και αν είναι αναγκαίο να αποτρέπει συγκεκριμένες ενέργειες πάνω στα κρίσιμα δεδομένα από έμπιστους τελικούς χρήστες.

Το σύστημα προστασίας δεδομένων από διαρροή θα πρέπει να εμποδίζει την απώλεια ευαίσθητων πληροφοριών, τη στιγμή της χρήσης τους (εννοώντας το περιβάλλον του τελικού χρήστη), ως αποτέλεσμα των ενεργειών του χρήστη, όπως: παράνομη αντιγραφή σε οπτικά ή αλλά εξωτερικά αποθηκευτικά μέσα π.χ. USB/ flash disks, εκτύπωση, μεταφορά μέσω δικτύου, ή αποστολή μέσω ηλεκτρονικού ταχυδρομείου. Επιπλέον θα πρέπει να παρακολουθεί συνεχώς τη ροή των πληροφοριών και τη χρήση εφαρμογών εμποδίζοντας τη διαρροή πληροφοριών εκτός του οργανισμού και εντοπίζοντας της ύπαρξη κακόβουλου λογισμικού.

Διαχείριση Ρίσκου (Risk Assessment/Treatment)

Στόχος των υπηρεσιών Risk Assessment (RA) είναι η αξιολόγηση καθώς και αποτίμηση των ρίσκων ασφάλειας καθώς συμπεριλαμβάνει όλες τις απειλές, ευπάθειες και τεχνικά μέτρα (υφιστάμενα ή σχεδιασμένα) με βάση πρότυπα όπως ISO27001/BIMCO/NIST/ISO22301 κ.λπ. 1ης φάσης είναι η ανάλυση της τρέχουσας κατάστασης των πληροφοριακών συστημάτων και δικτυακών υποδομών, των υφιστάμενων πολιτικών IT, διαδικασιών και πρακτικών IT, οι οποίες σχετίζονται με την ασφάλεια των πληροφοριών, την επιχειρησιακή συνέχεια και την προστασία των δεδομένων & εφαρμογών.

Ανάλυση Απειλών (Threat Analysis): Θα εξεταστούν οι εν δυνάμει απειλές προς τους πληροφοριακούς πόρους. Πιο συγκεκριμένα, στο στάδιο αυτό υλοποιείται ανάλυση του προφίλ των απειλών στις οποίες είναι εκτεθειμένοι οι πληροφοριακοί πόροι, με βάση τις παρακάτω παραμέτρους, για τα τεχνικά controls που έχουν ήδη εφαρμοστεί:

- Τα ενεργά δίκτυα των συστημάτων.
- Οι τρόποι πρόσβασης.
- Το είδος και ο αριθμός των χρηστών με πρόσβαση στα συστήματα.
- Interfaces επικοινωνίας.
- Επικοινωνία συστημάτων μεταξύ τους και με τρίτα πληροφοριακά συστήματα (ΠΣ).
- Δικτυακά συστήματα ασφάλειας (π.χ. Firewalls).
- Εφαρμογές και συστήματα παραγωγής (π.χ. servers, βάσεις δεδομένων κ.λπ.).

Ανάλυση Αδυναμιών Αρχιτεκτονικής: Οι αδυναμίες σε επίπεδο αρχιτεκτονικής μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση σε δίκτυα, συστήματα, εφαρμογές και να παρακάμψουν τα υφιστάμενα μέτρα ασφάλειας. Καλύπτονται τα ακόλουθα:

- Διαχωρισμός Δικτυακής Τοπολογίας (Network Security Segregation, DMZ κ.λπ.).
- Καταγραφή & αξιολόγηση αρχιτεκτονικής συστημάτων Ασφάλειας.
- Καταγραφή & αξιολόγηση ασφάλειας περιμέτρου σε σχέση με τα εξωτερικά δίκτυα.
- Καταγραφή & αξιολόγηση ασφάλειας Κεντρικών Συστημάτων και εταιρικού Domain (Active Directory).
- Καταγραφή & αξιολόγηση ασφάλειας πρόσβασης στο Internet/mail & απομακρυσμένης πρόσβασης/VPN.
- Καταγραφή & αξιολόγηση των Δικαιωμάτων Πρόσβασης (NAC).

Ανάλυση & Διαχείριση Κινδύνων: Αξιολογείται η επίδραση της πιθανής απώλειας της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας για τα πληροφοριακά συστήματα. Η αναφορά θα περιλαμβάνει και τις απειλές/αδυναμίες ασφάλειας με την πιθανότητα εμφάνισής τους και το επίπεδο αδυναμιών των πόρων στις απειλές αυτές. Το Σχέδιο Διαχείρισης Κινδύνου (Risk management) περιλαμβάνει τα προτεινόμενα αντίμετρα για τη διαχείριση κινδύνου, τα οποία θα περιγράψουν τον τρόπο βελτίωσης της ασφάλειας.

Η Cosmos Business Systems υποστηρίζει τους πελάτες σε όλες τις ανάγκες ασφάλειας.

COSMOS BUSINESS SYSTEMS AEBE TURN Key SOLUTIONS

COSMOS CONSULTING S.A.

CBS IT SYSTEMS CYPRUS LTD Member of Cosmos Business Systems Group, Greece TURN Key SOLUTIONS COMPANY

Αθήνα

Π. Μπακογιάννη 44, 144 52 Μεταμόρφωση, Αθήνα

☎ 210 6492800 🖷 210 6464069 ✉ cosmos@cbs.gr 🌐 www.cbs.gr

Θεσσαλονίκη

Θερμοκοιτίδα, Θέρμη 1, 9ο χλμ. Θεσσαλονίκης - Θέρμης, 570 01 Θεσσαλονίκη

☎ 2310 477670 🖷 2310 477672 ✉ cosmos.thess@cbs.gr 🌐 www.cbs.gr

Κύπρος

Λεωφ. Κένεντυ 81, 10 76 Λευκωσία, Κύπρος

☎ +357 22442101 🖷 +357 22313840

✉ sales@cbsit.com.cy 🌐 www.cbsit.com.cy