COSMOS
BUSINESS SYSTEMS AEBE

TURN Key SOLUTIONS

30 YEARS Your IT Business Partner

Η ΑΥΞΑΝΟΜΕΝΗ ΑΝΑΓΚΗ ΓΙΑ ΑΣΦΑΛΕΙΑ ΣΥΣΚΕΥΗΣ ΧΡΗΣΤΗ *(Endpoint)*

Η αύξηση στοχευμένων επιθέσεων και ransomware τα τελευταία χρόνια έχει καταστήσει πιο έντονα αναγκαία την διασφάλιση της συσκευής του χρήστη από απειλές. Επιπρόσθετα, ο κανονισμός GDPR είναι για κάθε εταιρεία υποχρεωτική προτεραιότητα που γεννάει ανάγκες για κρυπτογράφηση δεδομένων, ανίχνευση απειλών (threat discovery & forensics), data loss prevention και endpoint protection τεχνολογίες.

Οι τάσεις στην κυβερνοασφάλεια το 2019 συγκεντρώνονται γύρω από:

- Artificial Intelligence (AI) επιθέσεις και Machine Learning τεχνικές
- Κυβερνοπόλεμο ανάμεσα σε χώρες που είναι πια συχνό φαινόμενο
- Αύξηση των επιθέσεων ransomware
- Αύξηση στο crypto mining hijacking υπολογιστικής ισχύος σε υπολογιστές με την μορφή bitcoins ή άλλων cryptocurrency

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

Integrated Threat Detection and Defense
Endpoint Protection, E-mail Security, Sandboxing, Threat Intelligence, Behavioral Analysis

Securing Data and Applications
Endpoint Data Loss Prevention, Endpoint Encryption, προστασία σημαντικών εφαρμογών από απειλές και βελτίωση της απόδοσης τους (Application Isolation & Protection).

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 & forensics, disk/endpoint/email encryption, έλεγχο πρόσβασης σε εφαρμογές και δίκτυα καθώς και data classification/DLP.

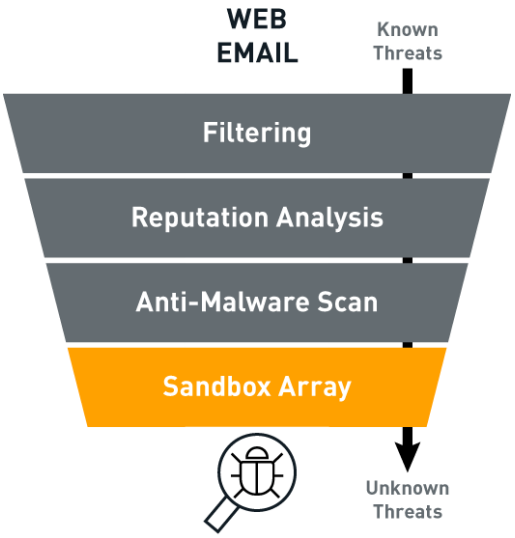
ΠΡΟΣΤΑΣΙΑ E-MAIL *(Endpoint)*

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.

ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΩΝ ΑΓΝΩΣΤΩΝ ΑΠΕΙΛΩΝ*(zero-day attacks/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.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Endpoint Encryption

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 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.

Endpoint DATA LOSS PREVENTION
(DLP)

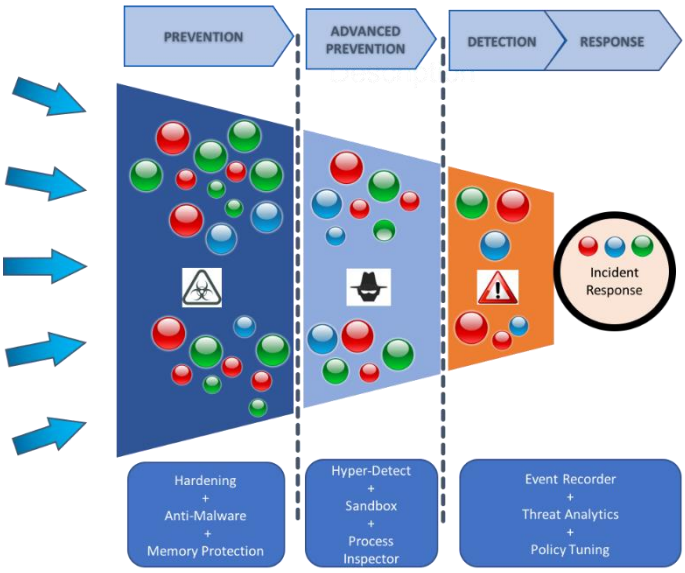
Η λύση DLP [Data Loss Prevention] είναι ένα σύστημα που εκτελεί ανίχνευση σε πραγματικό χρόνο των δεδομένων σε αποθήκευση και σε κίνηση, αξιολογεί δεδομένα που δεν πληρούν τις επικείμενες πολιτικές ασφάλειας, αναγνωρίζει παραβιάσεις πολιτικών και εφαρμόζει αυτόματα προεπιλεγμένες δράσεις όπως το να ενημερώνει τους χρήστες και τους διαχειριστές και να βάζει σε καραντίνα ύποπτους φακέλους, να κρυπτογραφεί δεδομένα ή να εμποδίζει ύποπτες κινήσεις.
Εν συντομία, η λύση DLP είναι ένα σετ από εργαλεία τεχνολογίας και διαδικασίες για να διασφαλιστεί ότι ευαίσθητα δεδομένα δεν θα χαθούν.
Εξαιτίας των κανονισμών του GDPR, όλο και περισσότερες εταιρείες επιλέγουν να εγκαταστήσουν DLP για να προστατέψουν ευαίσθητα δεδομένα από ατυχή χρήση (λάθος εργαζομένου) ή εγκληματική χρήση (παραβίαση από κυβερνοεπιθέσεις).
Οι εταιρείες εφαρμόζουν DLP για μία ποικιλία από λόγους όπως για να:

Διευθετήσουν τις προκλήσεις των δεδομένων σε χρήση, σε κίνηση και σε αποθήκευση.
Προστατέψουν τις θεσμικές, ιδιόκτητες και ευαίσθητες πληροφορίες από απειλές ασφάλειας που προκαλούνται από αυξημένη κινητικότητα εργαζομένων και τα νέα κανάλια επικοινωνίας
Αποτρέψουν την κακή χρήση των δεδομένων στις τερματικές συσκευές (desktops /laptops)
Οριοθετήσουν τις πολιτικές ασφαλείας με έτοιμες φόρμες πολιτικών

- Προστατέψουν δεδομένα στο Email Gateway στο cloud
- Έχουν διαχείριση δικτύου σε πραγματικό χρόνο
- Υποστηρίξουν συμμόρφωση με κανονισμούς με έτοιμες φόρμες για ευκολία.

Endpoint Detection & Response *(EDR)*

Σε πολλές περιπτώσεις η μόλυνση από malware είναι μεγαλύτερης έκτασης από ότι αρχικά ανιχνεύεται. Επίσης η αναζήτηση του υπεύθυνου για την επίθεση (χώρα προέλευσης, είδος επίθεσης κλπ.) δεν είναι συχνά προτεραιότητα με αποτέλεσμα να μην ολοκληρώνεται η κάθαρση του δικτύου μετά από μία επίθεση. Γνωρίζοντας και τα παραπάνω στοιχεία μας βοηθά να ανακαλύψουμε κρυμμένες μολύνσεις malware κ να βελτιώσουμε την άμυνα μας για την επόμενη επίθεση από τον ίδιο hacker.
Ο μηχανισμός αυτός αναζήτησης αποκαλύπτει πολύπλοκες επιθέσεις μέσω machine learning, user behavior analytics & threat intelligence ώστε να περιορίζονται τα false positives και να αποκαλύπτεται το εύρος της μόλυνσης πολύ γρηγορότερα.



Έτσι η λίστα των μολυσμένων συστημάτων αποκαλύπτεται άμεσα, κατά την αναζήτηση των ευρημάτων (και μετά από κάθε συμβάν). Η συμπεριφορά του χρήστη αναλύεται συνεχώς σε πραγματικό χρόνο, σε επίπεδο πρόσβασης τοπικών αρχείων, registry, logins, PowerShell και memory. Επιπλέον, κάθε νέα κρυμμένη ευπάθεια που έχει ξεφύγει από το basic malware protection και μολύνει κάποιο επιπλέον σύστημα, ανακαλύπτεται και μπαίνει στην blacklist (IP address, χώρα, νέο signature κλπ.. Όλα τα παραπάνω από έναν μοναδικό agent που εκτελεί και το basic virus protection.

Application Isolation & Control

Οι νέες μορφές επιθέσεων δεν χρησιμοποιούν ούτε κατεβάζουν εκτελέσιμα ή άλλου είδους αρχεία οπότε οι τεχνικές που βασίζονται σε αυτά δεν είναι αποτελεσματικές. Οι επιθέσεις αυτές εκμεταλλεύονται ευπάθειες στις εφαρμογές που ήδη υπάρχουν στην συσκευή κ επιτίθενται στην μνήμη/registry.
Με την προηγμένη αυτή λύση προστασίας και άμυνας οι ύποπτες εφαρμογές εκτελούνται σε προστατευμένο περιβάλλον. Αλλά ακόμα και τις εφαρμογές που εμπιστευόμαστε μπορούμε να τις εκτελέσουμε χωρίς επεμβάσεις και αλλοιώσεις από μολυσμένο κώδικα (trusted application shield).

Άλλωστε οι εφαρμογές που εμπιστευόμαστε είναι κ ο ποιο συνηθισμένος στόχος τέτοιας επίθεσης καθώς πολύ πιθανά να μην ελεγχθεί από συμβατικά εργαλεία. Το “Application Control & Isolation” αξιολογεί όλες τις εφαρμογές του χρήστη σε πραγματικό χρόνο (real time risk classification) και έτσι εμποδίζει την εκμετάλλευση τους από γνωστές ευπάθειες (application hardening). Επιπλέον, είναι εφικτό να εκτελεστούν μόνο γνωστές κ εγκεκριμένες εφαρμογές ενώ οι υπόλοιπες εμποδίζονται σε πραγματικό χρόνο αποφεύγοντας μολύνσεις από λάθος ή κακόβουλη ενέργεια.

Public Wi-Fi security defense

Μία από τις τακτικές επίθεσης κακόβουλων hackers είναι κ το στήσιμο ελεύθερων wi-fi δικτύων που να μοιάζουν με κάποια δημόσια εταιρικά (όπως internet café, εστιατόρια κλπ). Ο ανυποψίαστος χρήστης συνδέεται σε αυτά ώστε ο hacker να υποκλέψει συνομιλίες & κωδικούς.

Με την προστασία αυτή ο mobile user μπορεί να συνδεθεί άφοβα σε οποιοδήποτε δημόσιο ασύρματο δίκτυο καθώς αυτό ελέγχεται για την αξιοπιστία του (wi-fi network reputation & heuristics). Δημιουργείται σε πραγματικό χρόνο ένα εικονικό δίκτυο (VPN) αν ανιχνευτεί επίθεση ή σύνδεση με ύποπτη επικοινωνία. Αποφεύγονται έτσι man-in-the-middle επιθέσεις, κακόβουλα ελεύθερα wi-fi hotspots, κλπ μέσω ειδικής εφαρμογής που εγκαθίσταται στην συσκευή του χρήστη. Οι έλεγχοι που εφαρμόζονται αφορούν τα SSID που προβάλει το δίκτυο, οι ιδιότητες του wi-fi Access Point

WEB Site Protection & Isolation

Έχει παρατηρηθεί πως πολλά web sites δημιουργούνται για λίγα μόνο 24ωρα & αποκλειστικά για να μολύνουν ή να μεταφέρουν κακόβουλο λογισμικό στους χρήστες.
Επίσης αυξημένη είναι κ η χρήση των email phishing attacks έτσι ώστε ο χρήστης να παραδώσει στοιχεία στους hackers.
Η λειτουργία “user web isolation & security protection” προστατεύει τον χρήστη από μόλυνση περιεχομένου από γνωστά κακόβουλα sites, phishing campaigns & κλοπή στοιχείων σύνδεσης (credentials). Ταυτόχρονα επιτρέπει την απρόσκοπτη κ ασφαλή σύνδεση με άγνωστα sites ελέγχοντας τυχόν αρχεία, κείμενα & video που περιέχουν, πριν αυτά φτάσουν στον χρήστη.

Τα site αυτά αν κ ύποπτα ή άγνωστα δεν μπλοκάρονται απαραίτητα, επιτρέποντας την αυξημένη παραγωγικότητα των χρηστών.Η προστασία λειτουργεί σε κάθε internet browser και λειτουργικό σύστημα και εκμεταλλεύεται την γνωσιακή βάση του vendor στο Cloud. (πλήρως ενσωματωμένη στην λειτουργικότητα του βασικού antimalware agent).

SYMANTEC ENDPOINT : 2 UPGRADE STEPS - ΔΙΠΛΗ ΑΝΑΒΑΘΜΙΣΗ ΠΡΟΣΤΑΣΙΑΣ			
Desktop/laptop Protection Description	**Basic Endpoint Protection Features**	**Middle level Endpoint protection Features**	**Maximum level Endpoint Protection Features**
Basic antivirus protection (SEP) *	SEP Antivirus / Antispyware *		
zero day sandboxing protection		EDR (Detection & Response - Advanced Threat Protection)	
Application Control (Advanced Policies)		SEP-HAC - Application Control (Cloud-based)	
Advanced Sandboxing (shield Applications in protected environment)		SEP-HAI Application Isolation	
URL/surfing content inspection		WSS Basic Web Isolation (Proxy pac)	
encrypt local disk/usb disks			SEE Endpoint Encryption
Endpoint DLP (ban data file transfer to gmail, mail, copy/paste, etc)			Endpoint DLP (cloud & O365)
check public wi-fi networks for security before connecting			Endpoint Cloud Connect Defense (wi-fi secure vpn)

Basic antivirus protection με ενσωματωμένα τα:
network firewall (permit/deny TCP/UDP etc)
Device Control (on external devices usb sticks, BT, etc)
URL Filtering (Basic Whitelisting)
mail protection from attachements/ransome, etc
Application Control (basic whitelists)
Memory Mitigation zero-day inspection

Επικοινωνήστε με έναν από τους εξειδικευμένους σύμβουλους της **Cosmos Business Systems** για να σας συμβουλεύσουν σχετικά με τα προϊόντα, τα πλάνα και τον τρόπο αδειοδότησης, αλλά και να προτείνουν τη βέλτιστη λύση για τις σχεδιαστικές σας ανάγκες.

Άρης Χατζηπαπάς
Security Services Manager
hatjipapasa@cbs.gr

Τηλ. +30 210 6492800
Fax: +30 210 6464069

www.cbs.gr