CBS IT
SYSTEMS CYPRUS LTD
Member of Cosmos Business Systems Group, Greece

TURN Key
SOLUTIONS
COMPANY

Security Solutions

Your IT Business Partner

Η **CBS IT Systems Cyprus LTD**, ως ένας από τους μεγαλύτερους Systems Integrator της Κυπριακής αγοράς, παρέχει ολοκληρωμένες λύσεις και υπηρεσίες Ασφαλείας για την διασφάλιση των πληροφοριακών υποδομών και συστημάτων από απειλές. Επίσης με την πολυετή εμπειρία της, προσφέρει υπηρεσίες IT Consulting & Security Audit. Κατέχει πιστοποίηση ISO 9001 και απευθύνεται στην Κυπριακή αγορά των επιχειρήσεων και των επαγγελματιών – με έμφαση σε αυτή των μεσαίων και μεγάλων επιχειρήσεων του Ιδιωτικού και Δημόσιου τομέα, των Τραπεζών και των Τηλεπικοινωνιών.

Η **CBS IT Systems Cyprus LTD** ανήκει στον όμιλο Cosmos Business Systems, έναν από τους **μεγαλύτερους ομίλους τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών στην Ελλάδα και την Κύπρο.**

Οι λύσεις Ασφαλείας της CBS IT συγκαταλέγονται στις παρακάτω κατηγορίες:

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, 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.

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.

Στα πλαίσια υπηρεσιών βελτίωσης ασφάλειας IT υποδομής, η CBS IT παρέχει εξειδικευμένο λογισμικό για να καλύψει κάθε ανάγκη:

i) Endpoint based Solutions

- Antivirus (AV) / Endpoint Detection & Response (EDR)
- DLP

ii) Network Based Solutions

- UTM / NextGen Firewalls (physical & Virtual)
- Network Access Control (NAC)

iii) Cloud Based Solutions

- Mail Security (Cloud)
- MFA/SSO (Cloud)
- DNS Security (Cloud)
- WAF/DDOS/Load Balancers (Cloud)
- CASB (Cloud)

Επιπλέον παρέχει Security Consulting Services όπως:

- Security Audit, ICT Audit/Risk Assessment, DPOaaS, GDPR
- DLP, Audit, Policies, Intune, MFA, Conditional Access, Alerts
- Vulnerability Assessment (VA)

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 κυβερνο - ασφάλιση.
- Αύξηση στο crypto mining hijacking υπολογιστικής ισχύος σε υπολογιστές με την μορφή bitcoins ή άλλων cryptocurrency.
- Γενική έλλειψη ασφάλειας σε IoT συσκευές.

ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΥΜΒΑΙΝΟΥΝ ΣΕ ΟΛΑ ΤΑ ΕΙΔΗ ΕΤΑΙΡΕΙΩΝ

Μερικές από τις μεγαλύτερες επιθέσεις έγιναν σε πολύ γνωστές εταιρείες, με παραβιάσεις ασφαλείας που οδήγησαν στην κλοπή αρχείων, υποδηλώνοντας ότι κανείς δεν είναι ασφαλής.

Κοινωνικά Δίκτυα

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

Τομέας Υγείας

- Health South East, Νορβηγία Norway, 2.9 εκατομμύρια ιατρικά αρχεία.
- Under Armour, 150 εκατομμύρια ιατρικά δεδομένα συνδρομητών της εφαρμογής My-FitnessPal.

Τηλεπικοινωνιακοί Πάροχοι

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

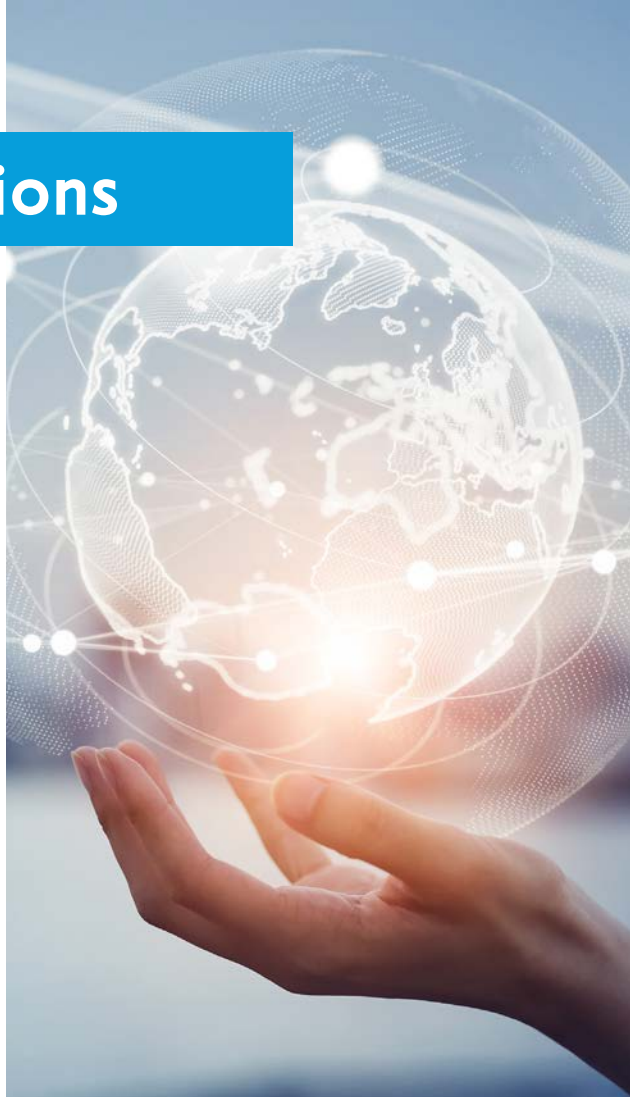
Επιχειρήσεις με ευαίσθητα δεδομένα

- Vtech Toys, 6.4 εκατομμύρια ονόματα, διευθύνσεις, φωτογραφίες παιδιών.
- Aetna Ασφαλιστική, 12,000 ιατρικοί φάκελοι ασθενών HIV με ονόματα και διευθύνσεις.

Τομέας Λιανικής Πώλησης

- eBay, 145 εκατομμύρια passwords, emails, user-names 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.

Endpoint based Solutions



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 κακόβουλη δραστηριότητα σε αυτά.

Καθώς περισσότερες επιχειρήσεις υιοθετούν πρακτικές BYOD (Bring Your Own Device) από εργαζόμενους (on premise ή remotely), η περίμετρος ασφάλειας του εταιρικού δικτύου κινδυνεύει με παραβίαση. Η ανάγκη για αποτελεσματική ασφάλεια στα τερματικά έχει αυξηθεί σημαντικά με την χρήση οικιακών υπολογιστών και laptop για σύνδεση στα εταιρικά δίκτυα.

Διαφοροποιώντας το endpoint security από τα λογισμικά antivirus τα endpoints χρήζουν ασφάλειας ατομικά. Οι λύσεις endpoint security πρέπει να έχουν λειτουργικότητα για:

- Detection & Response (EDR)
- Data Loss Prevention (DLP)
- Insider Threat Protection (ITP)
- Disk & Email encryption
- Έλεγχο πρόσβασης σε εφαρμογές και δίκτυα (NAC)
- Data classification
- Privileged access management (PAM)

Επιπρόσθετα στα user endpoints με την Cloud DNS Security προστασία οι internet συνδέσεις κάθε χρήστη (μέσω browser ή εφαρμογών) φιλτράρονται απομονώνοντας κακόβουλη επικοινωνία και εκτός εταιρικής περιμέτρου.

Τέλος, εφαρμόζοντας Zero Trust πολιτική, προτείνεται η εφαρμογή MFA/SSO ώστε να αποφευχθεί Identity Brute force attack σε υπηρεσίες και εφαρμογές εκτεθειμένες στο διαδίκτυο.

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.

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 διασφαλίζει την προστασία και παρακολούθηση της ροής των κρίσιμων δεδομένων μέσα και έξω από το «κλειστό» δίκτυο παραγωγής.

Network Based Solutions

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. 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.

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 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.

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.

- 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.

Cloud Based Security Solutions

MAIL SECURITY

Το ηλεκτρονικό ταχυδρομείο αποτελεί βασικό εργαλείο επικοινωνίας για τις επιχειρήσεις και ένα από τους βασικούς στόχους κυβερνοεπιθέσεων, καθώς είναι ένα εύκολο σημείο εισόδου σε λογαριασμούς και συσκευές.

Η **CBS IT** για την βελτίωση της ασφάλειας πληροφορίας στην υποδομή σας, προτείνει λύσεις προστασίας ηλεκτρονικού ταχυδρομείου από κακόβουλο περιεχόμενο.

Κύρια Χαρακτηριστικά των λύσεων mail server security:

Πολυεπίπεδη προστασία Anti-Spam / Anti-Malware

Οι παρακάτω τεχνικές που προσφέρουν οι λύσεις μας εντοπίζουν και αποκλείουν την πλειοψηφία των ανεπιθύμητων μηνυμάτων και με επιπλέον ανάλυση μέσω sandbox περιβάλλοντος: Έλεγχος πολλαπλών αποστολέων και περιεχομένου χρησιμοποιώντας έναν συνδυασμό από Domain Reputation Scores, URL filtering, Identity verifications, IP filtering, SPF, DKIM, DMARC και γεωγραφικούς περιορισμούς. Η δομή και το περιεχόμενο του μηνύματος αναλύονται με βάση τυχόν ψηφιακή υπογραφή, λέξεις-κλειδιά στο mail body, ανάλυση εικόνας, ενσωματωμένα web links και πιο προηγμένες τεχνικές όπως π.χ ανάλυση συμπεριφοράς και προστασία από ανεπιθύμητα μηνύματα.

Cloud & On-Premise επιλογές

Οι υλοποιήσεις των σχετικών συστημάτων προστασίας υποστηρίζονται on-premise αλλά και ON-Cloud. Προσφέρουν στον διαχειριστή αναλυτικές ημερήσιες αναφορές για τα κρίσιμα στατιστικά ασφάλειας των inboxes, κεντρική καραντίνα, διαχειριστές με ρόλους και αρμοδιότητες καθώς και πολύ γρήγορη αρχική εγκατάσταση.

MULTI FACTOR AUTHENTICATION (MFA) & SINGLE SIGN ON (SSO)

Με την χρήση των υπηρεσιών Multi Factor Authentication (MFA) & Single Sign On (SSO) ο χρήστης δημιουργεί μια ενιαία ιστοσελίδα η οποία περιέχει όλες τις συνδεδεμένες υπηρεσίας του (Dropbox, M365, Google services, κλπ). Η σύνδεση στη σελίδα γίνεται με έλεγχο της ταυτότητας και προσθήκη τρίτων παραγόντων αντί μόνο με username & password. Η ταυτοποίηση αυτή καλύπτει και τις υπόλοιπες συνδεδεμένες εφαρμογές ώστε η σύνδεση να είναι απλούστερη και ασφαλέστερη (Single Sign On – SSO). Αυξημένη ασφάλεια μπορεί να εφαρμοστεί και στις συνδέσεις των administrators στην IT υποδομή με την χρήση σε windows login RDP συνδέσεις και UAC requests για περιβάλλοντα windows 10 & windows servers.

Για όλες τις παραπάνω ενδεικτικές περιπτώσεις χρήσης, ο 3ος παράγοντας ταυτοποίησης (επιπλέον του username & password) μπορεί να είναι ένας από τους παρακάτω:

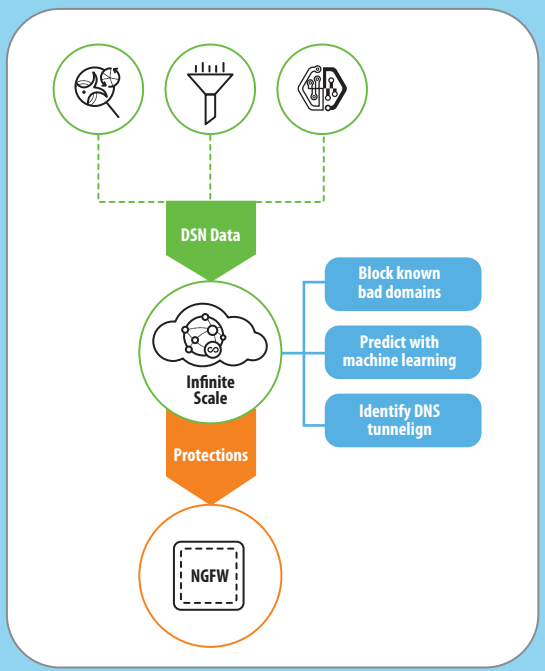
- Φυσικό Token 3ου κατασκευαστή
- Time Based One-Time Passcode-TOTP (επιπλέον κωδικό διάρκειας λίγων δευτερολέπτων)
- SMS passcode που λαμβάνεται στο κινητό όταν δεν υπάρχει internet access
- Push μηνύματοσμέσω ειδικής εφαρμογής στα κινητά

Με την χρήση επιπλέον optional agent η συσκευή είναι ασφαλής καθώς εφαρμόζονται ελέγχος (endpoint health checks), μειώνοντας το ρίσκο μόλυνσης.

Υποδομές με πάρα πολλούς χρήστες (σχολεία, ακαδημίες κλπ), μπορούν σαφώς να ωφεληθούν ακόμα περισσότερο, μειώνοντας δραστικά το διαχειριστικό χρόνο και κόστος, καθώς οι λύσεις μας συνδέονται και με το windows domain για συγκεντρωτική διαχείριση.

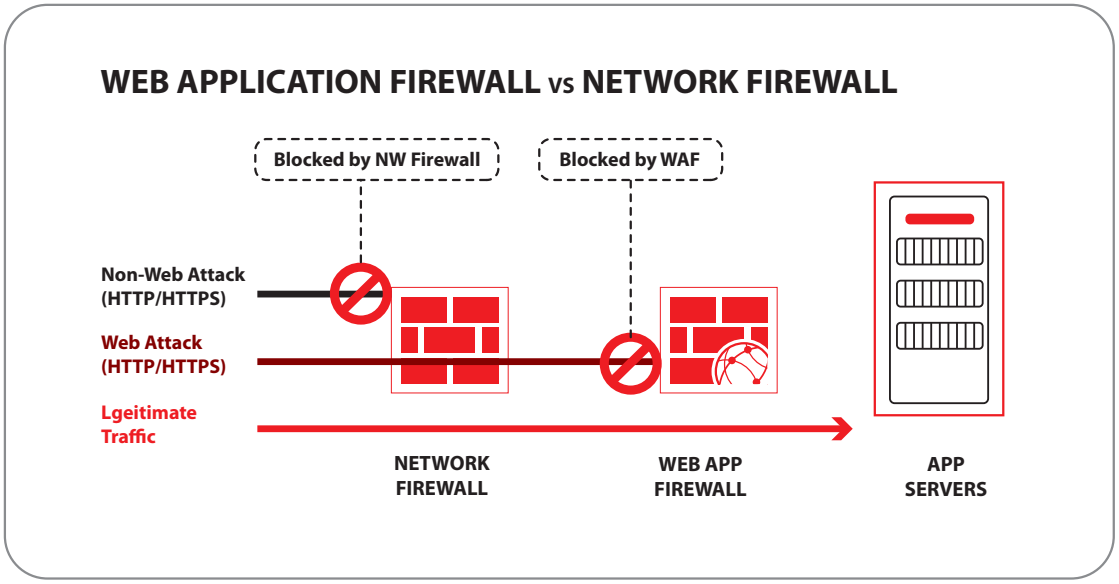
DNS SECURITY

Η **CBS IT** προτείνει λύσεις συνεργασίας με προμηθευτές που προσφέρουν ασφαλείς υπηρεσίες DNS, οι οποίες επιτρέπουν στους υπολογιστές σας να αναγνωρίζουν την επικίνδυνη δραστηριότητα DNS. Εφαρμόζουν πρωτόκολλα ασφαλείας που εμποδίζουν τις κακόβουλες συνδέσεις σε πραγματικό χρόνο σχετικά με κακόβουλο λογισμικό, email phishing, botnets και άλλες απειλές. Έτσι προστίθεται ένα πολύ αποτελεσματικό μέτρο DNS filtering στο επίπεδο DNS (δηλαδή το πρώτο βήμα για τη δημιουργία σύνδεσης). Μία επίθεση σταματά αν μπλοκαριστεί στο DNS layer.



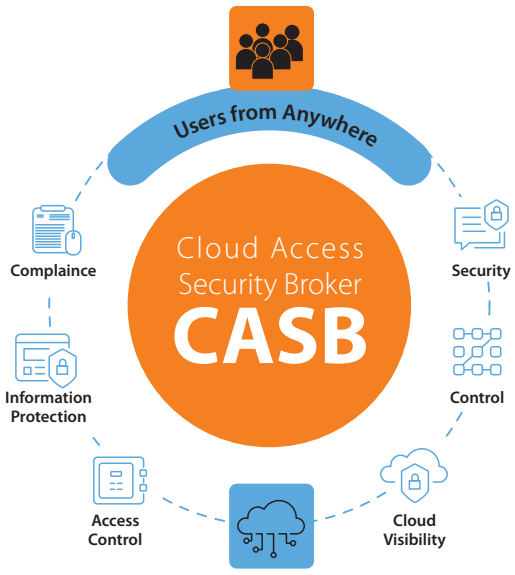
WEB APPLICATION FIREWALLS (WAF / DDOS / LOAD BALANCERS)

Η **CBS IT** προσφέρει λύσεις WAF / DDOS / CDN που τοποθετούν ένα Cloud layer προστασίας πριν η κακόβουλη κίνηση φτάσει στον εταιρικό Web Server. Οι λύσεις αυτές, διαφέρουν από τα Next Gen Firewalls καθώς επικεντρώνονται ειδικά σε web attacks και στην http/https επικοινωνία:



CLOUD ACCESS SECURITY BROKER (CASB)

Ο Cloud Access Security Broker (CASB) λειτουργεί σαν ενδιάμεσος μεταξύ των παρόχων Cloud services και των χρηστών έτσι ώστε η επικοινωνία τους να υλοποιείται με ασφάλεια. Οι λύσεις με αυτή την λειτουργικότητα πρέπει να προσφέρουν καταγραφή και ενημέρωση για τους συνδεδεμένους χρήστες (visibility), στατιστικά και Data Analytics για τον τρόπο χρήσης του Cloud, καθώς και έλεγχο πρόσβασης περιορίζοντας τον χρήστη με βάση τον ρόλο του.



Επιπρόσθετα το CASB επίπεδο καταγράφει όλες τις προσβάσιμες εφαρμογές ανά πάσα στιγμή (application visibility) με ταυτόχρονη κατηγοριοποίηση των δεδομένων τους (application classification). Όσες εφαρμογές εκθέτουν σε μεγάλο ρίσκο θα μπορούν να αποκλειστούν περιορίζοντας και τις περιπτώσεις διαρροής ευαίσθητων δεδομένων (CASB DLP).

Η **CBS IT** μπορεί να αξιολογήσει την κατάλληλη λύση CASB για την cloud υποδομή σας και να προσφέρει τις σχετικές άδειες σε συνδυασμό με την εφαρμογή προσαρμοσμένων πολιτικών ασφάλειας.

Consulting Services

Υπηρεσίες συμμόρφωσης με τον ευρωπαϊκό κανονισμό GDPR

- Ανάλυση της τρέχουσας κατάστασης ως προς την προστασία των προσωπικών δεδομένων, από την υφιστάμενη μελέτη GDPR
- Συμβουλευτικό και ενημερωτικό ρόλο προς τους υπεύθυνους ομάδων ή τμημάτων που επεξεργάζονται προσωπικά Δεδομένα.
- Παροχή οδηγιών και συμβουλών για τη συνεχή συμμόρφωση με τον κανονισμό (IT αλλά και έλεγχο εγγράφων)
- Συμμετοχή σε ομάδες εργασίας που αφορούν επεξεργασία ΠΔ
- Καθορισμό απαραίτητων ενεργειών για κάθε νέα διεργασία ή εφαρμογή, ενημέρωση του μητρώου ΠΔ και σύνταξη Μελέτης Εκτίμησης αντίκτυπου (Data Privacy Impact Assessment)
- Επικοινωνία και συνεργασία με την εποπτική αρχή (ΑΠΔΠΧ) για λογαριασμό του φορέα

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):** 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.

Vulnerability Assessment

Οι υπηρεσίες Vulnerability Assessment της **CBS IT** συμπεριλαμβάνουν:

► Αυτόματη αναζήτηση ευπαθειών στην IT υποδομή που περιλαμβάνει τα πληροφοριακά και δικτυακά συστήματα, και κάθε στοιχείο (asset) που είναι προσβάσιμο δικτυακά από ένα κεντρικό σημείο της υποδομής που θα μας υποδειχθεί. Σκοπός είναι να προσδιοριστεί το μέγεθος της ευπάθειας και απειλής παρέχοντας και τις απαραίτητες τεχνικές συμβουλές για την κάλυψη τους.

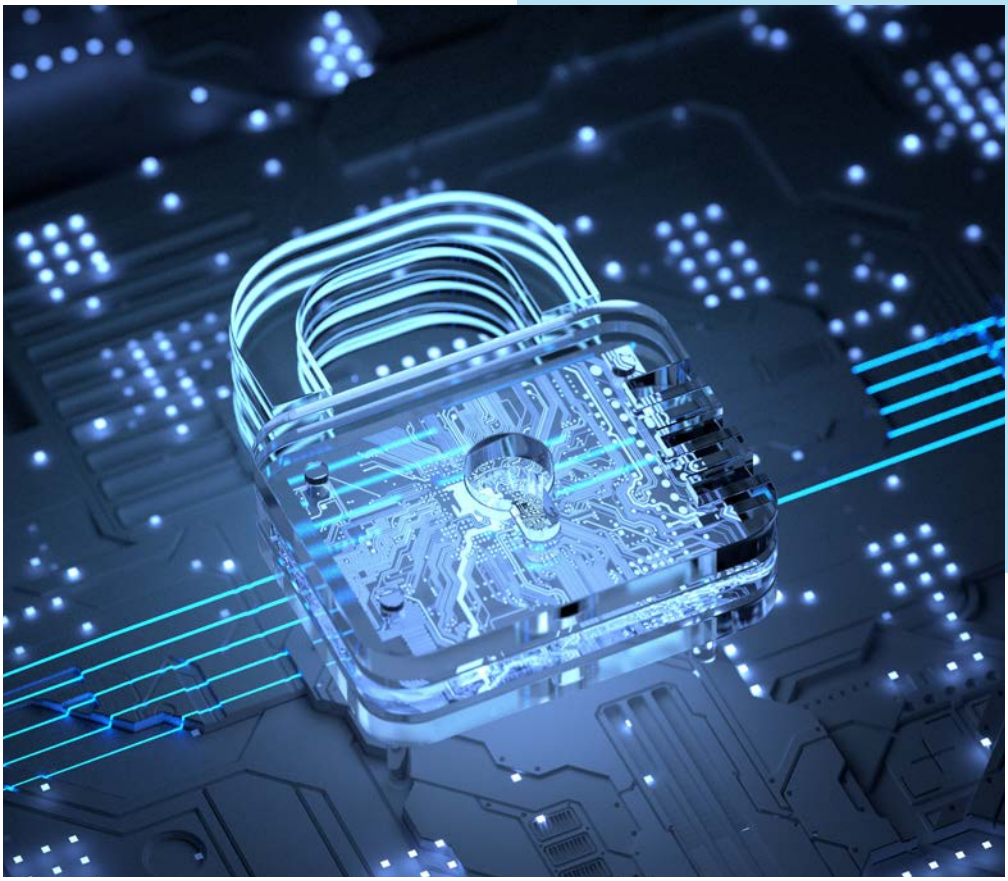
► Η υπηρεσία παρέχει στον υποψήφιο πελάτη αναλυτικό report των αποτελεσμάτων εσωτερικού ελέγχου ασφάλειας. Το report αυτό δημιουργείται από το εξειδικευμένο λογισμικό (Security Scanner) το οποίο ελέγχει κάθε σύστημα που ανακαλύπτει (αυτόματα) και βρίσκεται εγκατεστημένο σε εταιρικό laptop της **CBS IT**. Η όλη διαδικασία εφαρμόζεται σε windows & Linux συστήματα καθώς και σε δικτυακές συσκευές για network security audit.

► Η υπηρεσία μπορεί να προσφερθεί σε 6μηνιάια/ή ετήσια βάση ώστε να γίνονται περιοδικοί έλεγχοι με ανανεωμένη database με νεότερα ήδη attacks και να αξιολογούνται οι βελτιώσεις από τους προηγούμενους ελέγχους.

► Το λογισμικό θα επιχειρήσει να ανιχνεύσει τα παρακάτω (με την προϋπόθεση πλήρους πρόσβασης):

- Καταγραφή δικτυακής υποδομής (network mapping)
- Καταγραφή άλλων πληροφοριακών υποδομών (infrastructures mapping) όπως Directory Services Infrastructure, Groupware / Mail Infrastructure, κ.λπ.
- Καταγραφή συστημάτων (system mapping) & patch levels
- Καταγραφή συστημάτων ασφάλειας (security devices mapping)
- Καταγραφή εφαρμογών (application mapping) & port lists

► Μετά την ολοκλήρωση της αξιολόγησης θα δοθούν οι ευπάθειες που θα προκύψουν καθώς και τα απαραίτητα βήματα συμμόρφωσης (IT Gap Analysis). *(Στο συγκεκριμένο προϊόν δεν συμπεριλαμβάνεται η επίλυση των κενών ασφάλειας που θα υπάρξουν. Αυτές μπορούν να αξιολογηθούν και να δοθεί νέα προσφορά στον πελάτη με χρόνο και κόστος επίλυσης τους, όπου είναι εφικτό).*



CBS IT SYSTEMS CYPRUS LTD
Member of Cosmos Business Systems Group, Greece

TURN Key SOLUTIONS COMPANY

15 YEARS in CY

CYPRUS - CBS IT

Λεωφ. Κέννεντυ 81, Λευκωσία - 1076 Κύπρος
Τηλ.: +357 22442101 Fax: +357 22313840
email: sales@cbsit.com.cy
www.cbsit.com.cy

COSMOS BUSINESS SYSTEMS

Αθήνα: Τηλ.: +30 210 6492800, www.cbs.gr

cbscyprus cbs-it-systems-cyprus-ltd cbsitsystemscyprus