Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΑΠΕΙΛΩΝ **RANSOMWARE** ΜΕ ΟΠΛΟ ΤΗΝ **ΠΡΟΛΗΨΗ**

ΕΝΑΣ ΣΥΝΤΟΜΟΣ ΟΔΗΓΟΣ ΑΠΟ ΤΗ VERITAS

THINK PIECE BY **PERFORMANCE & VERITAS**

Think Ahead.

VERITAS

RANSOMWARE — Η ΟΜΗΡΕΙΑ ΠΟΥ ΜΠΟΡΕΙΤΕ ΝΑ ΠΡΟΛΑΒΕΤΕ

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που έχει σχεδιαστεί έτσι ώστε να απαγορεύει εκβιαστικά την πρόσβαση του χρήστη στα δεδομένα του, έως ότου αυτός ικανοποιήσει τις παράνομες και πολλές φορές, υπερβολικές, απαιτήσεις λύτρων αποδέσμευσης.

Στόχος των κυβερνο-εγκληματιών μπορεί να είναι οποιοσδήποτε. Είτε αυτή είναι μία μικρό-μεσαία επιχείρηση είτε ένας διεθνής οργανισμός.

Τα αποτελέσματα μιας τέτοιας επίθεσης μπορεί να είναι καταστροφικά και μπορεί να χτυπήσει οπουδήποτε τα δεδομένα.

Οι επιθέσεις μέσω ransomware, είναι τόσο διαδεδομένη απειλή που κάνει επιτακτική την ανάγκη να επικεντρωθούν οι επιχειρήσεις ακόμη περισσότερο στην ανάκαμψη μετά την επίθεση, ενώ ταυτόχρονα θα πρέπει να μειώσουν τον κίνδυνο μελλοντικών απειλών, προληπτικά.

Συνεπώς, η προετοιμασία του οργανισμού σας για μια επίθεση ransomware, γίνεται όλοένα και πιο κρίσιμη, μέρα με τη μέρα.

Το ransomware έχει αναδυθεί ταχύτατα τα τελευταία χρόνια και αποτελεί πλέον μία από τις σημαντικότερες κυβερνοαπειλές, τόσο για οργανισμούς όσο και για τελικούς χρήστες.

Σύμφωνα με τις εκτιμήσεις των ειδικών οι ζημιές —σε παγκόσμιο επίπεδο— είναι της τάξης των δισεκατομμυρίων € σε ετήσια βάση.

91%

των κυβερνοεπιθέσεων ξεκινούν με την τεχνική "spear-phishing", η οποία συχνά αφορά περιπτώσεις ransomware.

71%

των οργανισμών που δέχονται επιθέσεις ransomware φτάνουν τελικά να έχουν κάποιο επίπεδο «μόλυνσης».

$10k

Τα «λύτρα» φτάνουν εώς και $10 χιλ. ανά χρήστη. Η δε πληρωμή γίνεται σε κρυπτονόμισμα και είναι -συνεπώς μη ανιχνεύσιμη.

ΤΟ ΠΡΟΒΛΗΜΑ ΕΝ ΤΑΧΕΙ

Σύμφωνα με το Ransomware Resiliency Report της Veritas, δεν είναι πλέον θέμα το "αν", αλλά το "πότε" ένας οργανισμός θα αντιμετωπίσει μια σειρά απειλών από ransomware.

Η συγκεκριμένη έρευνα έδειξε ότι πολλές επιχειρήσεις μεταφέρουν περισσότερα από τα data και workloads, στο cloud, ωστόσο δεν είναι προετοιμασμένες όσο πρέπει.

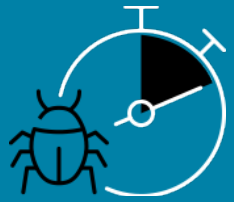
Πολλοί οργανισμοί παρουσιάζουν αδύνατα σημεία, τα λεγόμενα Resiliency Gaps, τα οποία θέτουν σε κίνδυνο τα δεδομένα και τη φήμη τους.

Με βάση το ίδιο report, το **42%** των IT leaders δήλωσε ότι οι εταιρείες τους **υπέστησαν επιθέσεις ransomware** και **δύο τρίτα** των ερωτηθέντων δήλωσαν ότι θα χρειαστούν περισσότερο από πέντε ημέρες για να ανακάμψουν πλήρως, γεγονός που σημαίνει ότι πολλοί από αυτούς αναγκάζονται να πληρώσουν επειδή κάθε λεπτό διακοπής λειτουργίας είναι πολύτιμο.

Επιπλέον, μόνο το ένα τρίτο των εταιρειών κρατούν δύο ή περισσότερα αντίγραφα των δεδομένων τους, ενώ δεν είναι σε θέση να τρέξουν γρήγορη και αποτελεσματική ανάκτηση.

Επιθέσεις ransomware

Το θέμα δεν είναι το αν, αλλά το πότε



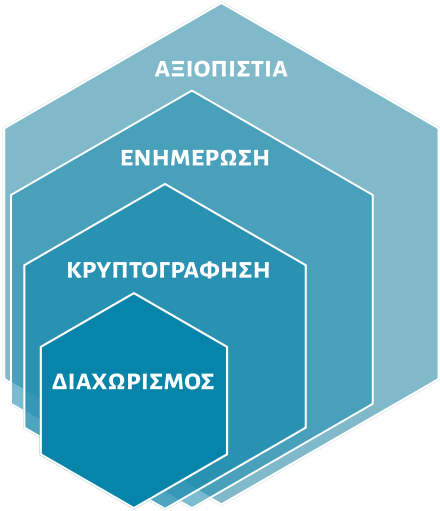
Κάθε 11 δευτερόλεπτα ένας οργανισμός δέχεται επίθεση ransomware

Είναι καιρός να ακολουθήσουμε μία προληπτική, ενοποιημένη προσέγγιση. Η Veritas μπορεί να σας βοηθήσει να **προστατέψετε** και να **ανακτήσετε** τα δεδομένα σας, ανεξάρτητα από το που βρίσκονται αυτά.

VERITAS: Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΜΕ ΟΠΛΟ ΤΗΝ ΠΡΟΛΗΨΗ

Θα πρέπει να διασφαλιστεί ότι οι επιχειρήσεις είναι έτοιμες να αντιμετωπίσουν τις κακόβουλες απειλές του σήμερα.

Η Veritas εστιάζει στο να καθοδηγήσει τους υπευθύνους για την ασφάλεια δεδομένων των οργανισμών, στην ανάπτυξη μιας προληπτικής προσέγγισης για την προστασία δεδομένων, σε συνδυασμό με ένα αξιόπιστο πρόγραμμα αποκατάστασης



Διαχωρισμός των αντιγράφων δεδομένων: Διατηρήστε τρία ή περισσότερα αντίγραφα δεδομένων σε διαφορετικές τοποθεσίες για να μειώσετε τις πιθανότητες πρόσβασης στο σύνολο των δεδομένων από έναν επίδοξο εισβολέα.

Αποθήκευση δεδομένων με ασφάλεια: Η κρυπτογράφηση των δεδομένων σας μπορεί να βοηθήσει στη ματαίωση των επιθέσεων καθιστώντας πιο δύσκολο για το ransomware να εντοπίσει ποια δεδομένα έχετε αποθηκεύσει.

Εάν ο αποθηκευτικός σας χώρος έχει παραβιαστεί, τα αρχεία που περιέχουν προσωπικά δεδομένα είναι πιο δύσκολο να κοινοποιηθούν στο διαδίκτυο, όταν είναι κρυπτογραφημένα, εμποδίζοντας τους εισβολείς να διανείμουν κρίσιμα δεδομένα ως μέρος ενός προγράμματος εκβιασμού.

Πρόληψη μέσα από τη ενημέρωση: Βεβαιωθείτε ότι οι εργαζόμενοι, σε όλους τους τομείς, κατανοούν την ανάγκη για καθημερινή ασφάλεια δεδομένων σε όλα τα επίπεδα IT.

Εφαρμογή αξιόπιστων λύσεων: Εφαρμόστε λύσεις που παρέχουν σαφή ασφάλεια στον οργανισμό, αξιόπιστη και έξυπνη προστασία δεδομένων, όπως το Veritas Enterprise Data Services Platform, σε συνδυασμό το NetBackup 9.

ΔΥΟ ΒΑΣΙΚΑ ΣΥΣΤΑΤΙΚΑ ΣΑΣ ΚΑΤΑ ΤΟΥ RANSOMWARE:

Veritas NetBackup: Το εμπιστεύεται 87% των Fortune Global 500, αλλά και η πλειοψηφία των μικρομεσαίων οργανισμών ανά τον κόσμο. Παρέχει ασφαλή backup σε πλατφόρμες Windows, UNIX και Linux και ενοποιημένη προστασία δεδομένων για virtual και physical περιβάλλοντα multi-cloud των οποίων η διαχείριση μπορεί να γίνει εύκολα, σε παγκόσμιο επίπεδο, από μία μόνο κονσόλα.

Enterprise Data Services Platform: Προσφέρει λύσεις στους τρεις τομείς που έχουν μεγαλύτερη βαρύτητα, ήτοι **availability**, **protection και insights**. Είναι η πιο ευέλικτη και επεκτάσιμη πλατφόρμα που διατίθεται στις επιχειρήσεις. Ενσωματώνει στον πυρήνα του το NetBackup και υποστηρίζει 500+ data sources, 150+ storage targets και 60+ clouds.

iOS
Apple iOS™

Windows
Microsoft Windows™

Android™

Linux™

Σημαντικό: Το ransomware αποτελεί απειλή για όλες τις γνωστές πλατφόρμες και λειτουργικά συστηματα.

VERITAS™

CYBERSECURITY AND
CONTINUITY SOLUTIONS

ARPIL — 2021

RANSOMWARE PROTECTION ΑΠΟ VERITAS & PERFORMANCE

A 'THINK PIECE' BY
PERFORMANCE & VERITAS

ΡΩΤΗΣΤΕ ΜΑΣ
210–9947100
info@performance.gr

performance