ΣΥΣΤΑΣΕΙΣ

ΣΥΣΤΑΣΗ (ΕΕ) 2019/553 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 3ης Απριλίου 2019

σχετικά με την κυβερνοασφάλεια στον τομέα της ενέργειας

[κοινοποιηθείσα υπό τον αριθμό C(2019) 2400]

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 292,

Εκτιμώντας τα ακόλουθα:

(1) Ο ευρωπαϊκός τομέας της ενέργειας διέρχεται μια σημαντική αλλαγή προς μια οικονομία χωρίς ανθρακούχες εκπομπές, με παράλληλη εγγύηση της ασφάλειας του εφοδιασμού και της ανταγωνιστικότητας. Στο πλαίσιο αυτής της ενεργειακής μετάβασης και της συναφούς αποκέντρωσης της παραγωγής ενέργειας από ανανεώσιμες πηγές, η τεχνολογική πρόοδος, η σύζευξη των τομέων και η ψηφιοποίηση μετατρέπουν το δίκτυο ηλεκτρικής ενέργειας της Ευρώπης σε «έξυπνο δίκτυο». Ταυτόχρονα, αυτό συνεπάγεται νέους κινδύνους, καθώς η ψηφιοποίηση καθιστά το ενεργειακό σύστημα ολοένα και πιο ευάλωτο σε κυβερνοεπιθέσεις και περιστατικά που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια του ενεργειακού εφοδιασμού.

(2) Η έκδοση του συνόλου των οκτώ νομοθετικών προτάσεων ([1]) της δέσμης μέτρων «Καθαρή ενέργεια για όλους τους Ευρωπαίους», συμπεριλαμβανομένης της διακυβέρνησης της Ενεργειακής Ένωσης ως εφαλτηρίου, επιτρέπει τη δημιουργία ευνοϊκού περιβάλλοντος για τον ψηφιακό μετασχηματισμό του ενεργειακού τομέα. Σε αυτήν αναγνωρίζεται επίσης η σημασία της κυβερνοασφάλειας στον τομέα της ενέργειας. Ειδικότερα, η αναδιατύπωση του κανονισμού σχετικά με την εσωτερική αγορά ηλεκτρικής ενέργειας ([2]) προβλέπει την έγκριση τεχνικών κανόνων για την ηλεκτρική ενέργεια, όπως του κώδικα δικτύου σχετικά με ειδικούς ανά τομέα κανόνες για τις πτυχές κυβερνοασφάλειας των διασυνοριακών ροών ηλεκτρικής ενέργειας, για τις κοινές ελάχιστες απαιτήσεις, τον σχεδιασμό, την παρακολούθηση, την υποβολή εκθέσεων και τη διαχείριση κρίσεων. Ο κανονισμός σχετικά με την ετοιμότητα αντιμετώπισης κινδύνων στον τομέα της ηλεκτρικής ενέργειας ([3]) ακολουθεί σε γενικές γραμμές την προσέγγιση που επιλέχθηκε στον κανονισμό για την ασφάλεια του εφοδιασμού με φυσικό αέριο ([4])· τονίζει την ανάγκη ορθής εκτίμησης όλων των κινδύνων, συμπεριλαμβανομένων εκείνων που σχετίζονται με την κυβερνοασφάλεια, και προτείνει τη λήψη μέτρων πρόληψης και μετριασμού των κινδύνων που έχουν εντοπιστεί.

(3) Όταν η Επιτροπή ενέκρινε τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο ([5]) το 2013, προσδιόρισε ως προτεραιότητα την ενίσχυση της κυβερνοανθεκτικότητας της Ένωσης. Ένα από τα βασικά παραδοτέα της στρατηγικής είναι η οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών ([6]) (εφεξής «οδηγία NIS»), η οποία εκδόθηκε τον Ιούλιο του 2016. Ως πρώτη πράξη της οριζόντιας νομοθεσίας της ΕΕ για την κυβερνοασφάλεια, η οδηγία NIS ενισχύει το συνολικό επίπεδο κυβερνοασφάλειας στην Ένωση μέσω της ανάπτυξης εθνικών ικανοτήτων κυβερνοασφάλειας, της αύξησης της συνεργασίας σε επίπεδο ΕΕ και της θέσπισης υποχρεώσεων υποβολής εκθέσεων σχετικά με την ασφάλεια και τα περιστατικά για εταιρείες που αναφέρονται ως «φορείς εκμετάλλευσης βασικών υπηρεσιών». Η αναφορά περιστατικών είναι υποχρεωτική σε βασικούς τομείς, συμπεριλαμβανομένου του τομέα της ενέργειας.

([1]) Οδηγία (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για την προώθηση της χρήσης ενέργειας από ανανεώσιμες πηγές (ΕΕ L 328 της 21.12.2018, σ. 82)· οδηγία (ΕΕ) 2018/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, σχετικά με την τροποποίηση της οδηγίας 2012/27/ΕΕ για την ενεργειακή απόδοση (ΕΕ L 328 της 21.12.2018, σ. 210)· κανονισμός (ΕΕ) 2018/1999 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη διακυβέρνηση της Ενεργειακής Ένωσης και της Δράσης για το Κλίμα, για την τροποποίηση των κανονισμών (ΕΚ) αριθ. 663/2009 και (ΕΚ) αριθ. 715/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, των οδηγιών 94/22/ΕΚ, 98/70/ΕΚ, 2009/31/ΕΚ, 2009/73/ΕΚ, 2010/31/ΕΕ, 2012/27/ΕΕ και 2013/30/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, των οδηγιών 2009/119/ΕΚ και (ΕΕ) 2015/652 του Συμβουλίου και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 525/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 328 της 21.12.2018, σ. 1)· οδηγία (ΕΕ) 2018/844 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2018, για την τροποποίηση της οδηγίας 2010/31/ΕΕ για την ενεργειακή απόδοση των κτιρίων και της οδηγίας 2012/27/ΕΕ για την ενεργειακή απόδοση (ΕΕ L 156 της 19.6.2018, σ. 75). Το Ευρωπαϊκό Κοινοβούλιο, κατά τη σύνοδο ολομέλειας του Μαρτίου του 2019, επιβεβαίωσε τις πολιτικές συμφωνίες που επιτεύχθηκαν με το Συμβούλιο σχετικά με τις προτάσεις σχεδιασμού της αγοράς ηλεκτρικής ενέργειας (κανονισμός για την ετοιμότητα αντιμετώπισης κινδύνων, κανονισμός για τον Οργανισμό Συνεργασίας των Ρυθμιστικών Αρχών Ενέργειας (ACER), καθώς και την οδηγία για την ηλεκτρική ενέργεια και τον κανονισμό για την ηλεκτρική ενέργεια. Η επίσημη έγκριση από το Συμβούλιο αναμένεται να πραγματοποιηθεί τον Απρίλιο· η δημοσίευση του νομικού κειμένου στην ΕΕ θα ακολουθήσει αμέσως μετά.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Κανονισμός (ΕΕ) 2017/1938 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2017, σχετικά με τα μέτρα κατοχύρωσης της ασφάλειας εφοδιασμού με αέριο και με την κατάργηση του κανονισμού (ΕΕ) αριθ. 994/2010 (ΕΕ L 280 της 28.10.2017, σ. 1).

([5]) JOIN(2013) 1.

([6]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

(4) Κατά την εφαρμογή μέτρων ετοιμότητας στον τομέα της κυβερνοασφάλειας, τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των φορέων εκμετάλλευσης βασικών υπηρεσιών στον τομέα της ενέργειας, όπως αυτά προσδιορίζονται βάσει της οδηγίας NIS, θα πρέπει να λαμβάνουν υπόψη τις οριζόντιες κατευθυντήριες γραμμές που εκδίδει η ομάδα συνεργασίας NIS, η οποία έχει συσταθεί βάσει του άρθρου 11 της οδηγίας NIS. Η εν λόγω ομάδα συνεργασίας, η οποία απαρτίζεται από εκπροσώπους των κρατών μελών, του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) και της Επιτροπής, έχει εκδώσει έγγραφα καθοδήγησης σχετικά με τα μέτρα ασφάλειας και την κοινοποίηση συμβάντων. Τον Ιούνιο του 2018, η εν λόγω ομάδα δημιούργησε έναν ειδικό άξονα δράσης για την ενέργεια.

(5) Στην κοινή ανακοίνωση για την κυβερνοασφάλεια του 2017 ([7]) αναγνωρίζεται η σημασία των ειδικών ανά τομέα παραμέτρων και απαιτήσεων σε επίπεδο ΕΕ, μεταξύ άλλων και του τομέα της ενέργειας. Η κυβερνοασφάλεια και οι πιθανές επιπτώσεις στις πολιτικές έχουν αποτελέσει αντικείμενο εκτεταμένης διαδικασίας συζήτησης στην Ένωση κατά τα τελευταία έτη. Κατά συνέπεια, υπάρχει σήμερα αυξανόμενη συνειδητοποίηση ότι οι επιμέρους οικονομικοί τομείς αντιμετωπίζουν ειδικά ζητήματα κυβερνοασφάλειας και, ως εκ τούτου, πρέπει να αναπτύξουν τις δικές τους τομεακές προσεγγίσεις εντός του ευρύτερου πλαισίου των γενικών στρατηγικών κυβερνοασφάλειας.

(6) Η ανταλλαγή πληροφοριών και η εμπιστοσύνη αποτελούν βασικά στοιχεία της κυβερνοασφάλειας. Η Επιτροπή σκοπεύει να αυξήσει την ανταλλαγή πληροφοριών μεταξύ των σχετικών ενδιαφερόμενων φορέων διοργανώνοντας ειδικές εκδηλώσεις, όπως για παράδειγμα η υψηλού επιπέδου συζήτηση στρογγυλής τράπεζας για την κυβερνοασφάλεια που διοργανώθηκε στη Ρώμη τον Μάρτιο του 2017 και η υψηλού επιπέδου διάσκεψη για την κυβερνοασφάλεια που διοργανώθηκε στις Βρυξέλλες τον Οκτώβριο του 2018. Η Επιτροπή επιθυμεί επίσης να ενισχύσει τη συνεργασία μεταξύ των σχετικών ενδιαφερόμενων και των ειδικευμένων φορέων, όπως το Ευρωπαϊκό Κέντρο Ανταλλαγής και Ανάλυσης των Πληροφοριών για την Ενέργεια.

(7) Ο κανονισμός για τον ENISA, τον «Οργανισμό κυβερνοασφάλειας της ΕΕ», και για την πιστοποίηση της κυβερνοασφάλειας των τεχνολογιών πληροφοριών και επικοινωνιών («κανονισμός για την κυβερνοασφάλεια») ([8]) θα ενισχύσει την εντολή του Οργανισμού κυβερνοασφάλειας της ΕΕ, ώστε αυτός να στηρίξει καλύτερα τα κράτη μέλη στην αντιμετώπιση των απειλών και των επιθέσεων κυβερνοασφάλειας. Δημιουργεί επίσης ένα ευρωπαϊκό πλαίσιο κυβερνοασφάλειας για την πιστοποίηση προϊόντων, διαδικασιών και υπηρεσιών, το οποίο θα ισχύει σε ολόκληρη την Ένωση και παρουσιάζει ιδιαίτερο ενδιαφέρον για τον τομέα της ενέργειας.

(8) Η Επιτροπή διατύπωσε σύσταση ([9]) για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας στην 5η γενιά (5G) τεχνολογιών δικτύου με τον καθορισμό κατευθυντήριων γραμμών για την κατάλληλη ανάλυση των κινδύνων και τα μέτρα διαχείρισης της επικινδυνότητας σε εθνικό επίπεδο, για την ανάπτυξη μιας συντονισμένης ευρωπαϊκής ανάλυσης της επικινδυνότητας και για την καθιέρωση διαδικασίας για την ανάπτυξη κοινής εργαλειοθήκης με τα βέλτιστα μέτρα διαχείρισης της επικινδυνότητας. Μετά την εισαγωγή τους, τα δίκτυα 5G θα αποτελέσουν τον κορμό ενός ευρέος φάσματος υπηρεσιών, απαραίτητων για τη λειτουργία της εσωτερικής αγοράς και για την εκτέλεση ζωτικών κοινωνικών και οικονομικών λειτουργιών – όπως η ενέργεια.

(9) Η παρούσα σύσταση θα πρέπει να παρέχει μη εξαντλητική καθοδήγηση στα κράτη μέλη και στους σχετικούς ενδιαφερόμενους φορείς, ιδίως στους διαχειριστές δικτύων και στους προμηθευτές τεχνολογίας, για την επίτευξη υψηλότερου επιπέδου κυβερνοασφάλειας δεδομένων των ειδικών απαιτήσεων πραγματικού χρόνου που έχουν προσδιοριστεί για τον τομέα της ενέργειας, των αλυσιδωτών επιπτώσεων και του συνδυασμού κληροδοτημένων τεχνολογιών με τεχνολογίες αιχμής. Σκοπός του παρόντος εγγράφου είναι να βοηθήσει τους ενδιαφερόμενους φορείς να λαμβάνουν υπόψη τις ειδικές απαιτήσεις του τομέα της ενέργειας κατά την εφαρμογή διεθνώς αναγνωρισμένων προτύπων κυβερνοασφάλειας ([10]).

(10) Η Επιτροπή προτίθεται να επανεξετάζει τακτικά την παρούσα σύσταση με βάση την πρόοδο που σημειώνεται σε ολόκληρη την Ένωση, σε διαβούλευση με τα κράτη μέλη και τους σχετικούς ενδιαφερόμενους φορείς. Η Επιτροπή θα συνεχίσει τις προσπάθειές της για την ενίσχυση της κυβερνοασφάλειας στον τομέα της ενέργειας, ιδίως μέσω της ομάδας συνεργασίας NIS, η οποία διασφαλίζει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών στον τομέα της κυβερνοασφάλειας,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΣΤΑΣΗ:

ΑΝΤΙΚΕΙΜΕΝΟ

1) Η παρούσα σύσταση καθορίζει τα κύρια ζητήματα που σχετίζονται με την κυβερνοασφάλεια στον τομέα της ενέργειας, συγκεκριμένα τις απαιτήσεις πραγματικού χρόνου, τις αλυσιδωτές επιπτώσεις και τον συνδυασμό της κληροδοτημένης τεχνολογίας με την τεχνολογία αιχμής, και προσδιορίζει τις κύριες δράσεις για την εφαρμογή σχετικών μέτρων ετοιμότητας για την κυβερνοασφάλεια στον τομέα της ενέργειας.

([7]) JOIN(2017) 450.

([8]) Η πράξη για την κυβερνοασφάλεια εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο τον Μάρτιο του 2019. Η επίσημη έγκριση από το Συμβούλιο αναμένεται να πραγματοποιηθεί τον Απρίλιο· η δημοσίευση του νομικού κειμένου στην ΕΕ θα ακολουθήσει αμέσως μετά.

([9]) C(2019) 2335.

([10]) Οι διεθνείς οργανισμοί τυποποίησης έχουν δημοσιεύσει διάφορα πρότυπα κυβερνοασφάλειας (ISO/IEC 27000: Τεχνολογίες πληροφοριών) και διαχείρισης κινδύνων (ISO/IEC31000: Εφαρμογή της διαχείρισης κινδύνων). Ένα ειδικό πρότυπο για τον τομέα της ενέργειας (ISO/IEC 27019: έλεγχοι της ασφάλειας των πληροφοριών για τον κλάδο των υπηρεσιών κοινής ωφελείας στον τομέα της ενέργειας) εκδόθηκε στο πλαίσιο των σειρών ISO/IEC 27000 του Οκτωβρίου του 2017.

2) Κατά την εφαρμογή της παρούσας σύστασης, τα κράτη μέλη θα πρέπει να ενθαρρύνουν τους σχετικούς ενδιαφερόμενους φορείς να αναπτύξουν γνώσεις και δεξιότητες που σχετίζονται με την κυβερνοασφάλεια στον τομέα της ενέργειας. Κατά περίπτωση, τα κράτη μέλη θα πρέπει να συμπεριλάβουν τα θέματα αυτά στο εθνικό τους πλαίσιο κυβερνοασφάλειας, ιδίως μέσω στρατηγικών, νομοθετημάτων, κανονιστικών και άλλων διοικητικών διατάξεων.

ΑΠΑΙΤΗΣΕΙΣ ΠΡΑΓΜΑΤΙΚΟΥ ΧΡΟΝΟΥ ΤΩΝ ΣΥΝΙΣΤΩΣΩΝ ΤΩΝ ΕΝΕΡΓΕΙΑΚΩΝ ΥΠΟΔΟΜΩΝ

3) Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα σχετικά ενδιαφερόμενα μέρη, ιδίως οι διαχειριστές δικτύων ενέργειας και οι πάροχοι τεχνολογίας, και ιδίως οι φορείς εκμετάλλευσης βασικών υπηρεσιών που προσδιορίζονται στην οδηγία NIS, εφαρμόζουν τα σχετικά μέτρα ετοιμότητας στον τομέα της κυβερνοασφάλειας που σχετίζονται με τις απαιτήσεις πραγματικού χρόνου στον τομέα της ενέργειας. Ορισμένα στοιχεία του ενεργειακού συστήματος πρέπει να λειτουργούν σε «πραγματικό χρόνο», δηλαδή να αντιδρούν σε εντολές εντός λίγων χιλιοστών του δευτερολέπτου, γεγονός που καθιστά δύσκολη ή ακόμη και αδύνατη τη λήψη μέτρων κυβερνοασφάλειας, λόγω έλλειψης χρόνου.

4) Ειδικότερα, οι διαχειριστές δικτύων ενέργειας θα πρέπει:

α) να εφαρμόζουν, όπου ενδείκνυται, τα πλέον πρόσφατα πρότυπα ασφαλείας για νέες εγκαταστάσεις και να εξετάζουν τη λήψη συμπληρωματικών μέτρων υλικής ασφάλειας, στις περιπτώσεις στις οποίες οι υφιστάμενες παλαιές εγκαταστάσεις δεν μπορούν να προστατευτούν επαρκώς με μηχανισμούς κυβερνοασφάλειας·

β) να εφαρμόζουν διεθνή πρότυπα κυβερνοασφάλειας και επαρκή ειδικά τεχνικά πρότυπα ασφαλούς επικοινωνίας σε πραγματικό χρόνο αμέσως μόλις τα αντίστοιχα προϊόντα καταστούν διαθέσιμα στο εμπόριο·

γ) να εξετάζουν τους περιορισμούς πραγματικού χρόνου στη συνολική προσέγγιση ασφάλειας των περιουσιακών στοιχείων, ιδίως όσον αφορά την κατάταξη των περιουσιακών στοιχείων·

δ) να εξετάζουν τα καθεστώτα τηλεπροστασίας των ιδιόκτητων δικτύων από την άποψη των περιορισμών πραγματικού χρόνου, ώστε να διασφαλίζεται η απαιτούμενη ποιότητα υπηρεσίας· όταν χρησιμοποιούν δημόσια δίκτυα επικοινωνιών, οι φορείς εκμετάλλευσης θα πρέπει να εξασφαλίζουν ειδική εκχώρηση εύρους ζώνης, απαιτήσεις χρόνου αναμονής και μέτρα ασφάλειας των επικοινωνιών·

ε) να διασπούν το συνολικό σύστημα σε λογικές ζώνες και, εντός κάθε ζώνης, να θεσπίζουν χρονικούς και διαδικαστικούς περιορισμούς, ώστε να καθίσταται δυνατή η εφαρμογή κατάλληλων μέτρων κυβερνοασφάλειας ή να εξετάζουν εναλλακτικές μεθόδους προστασίας.

5) Κατά περίπτωση, οι διαχειριστές δικτύων ενέργειας θα πρέπει επίσης:

α) να επιλέγουν ένα ασφαλές πρωτόκολλο επικοινωνίας, λαμβάνοντας υπόψη τις απαιτήσεις πραγματικού χρόνου, για παράδειγμα μεταξύ μιας εγκατάστασης και των συστημάτων διαχείρισής της (Σύστημα ενεργειακής διαχείρισης – EMS/ Σύστημα διαχείρισης της διανομής – DMS)·

β) να θεσπίσουν κατάλληλο μηχανισμό επαλήθευσης της ταυτότητας για την επικοινωνία μηχανής με μηχανή, με σκοπό την αντιμετώπιση των απαιτήσεων πραγματικού χρόνου.

ΑΛΥΣΙΔΩΤΕΣ ΕΠΙΠΤΩΣΕΙΣ

6) Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα σχετικά ενδιαφερόμενα μέρη, κατ' εξοχήν οι διαχειριστές δικτύων ενέργειας και οι πάροχοι τεχνολογίας, και ιδίως οι φορείς εκμετάλλευσης βασικών υπηρεσιών που προσδιορίζονται βάσει της οδηγίας NIS, εφαρμόζουν τα σχετικά μέτρα ετοιμότητας στον τομέα της κυβερνοασφάλειας που σχετίζονται με τις αλυσιδωτές επιπτώσεις στον τομέα της ενέργειας. Τα δίκτυα ηλεκτρικής ενέργειας και οι αγωγοί φυσικού αερίου αλληλοσυνδέονται στενά σε ολόκληρη την Ευρώπη και μια κυβερνοεπίθεση που δημιουργεί μη διαθεσιμότητα ή διακοπή σε ένα τμήμα του ενεργειακού συστήματος μπορεί να πυροδοτήσει εκτεταμένες αλυσιδωτές επιπτώσεις σε άλλα τμήματα του εν λόγω συστήματος.

7) Κατά την εφαρμογή της παρούσας σύστασης, τα κράτη μέλη θα πρέπει να αξιολογούν τις αλληλεξαρτήσεις και την κρισιμότητα της ηλεκτροπαραγωγής και τα συστήματα ευέλικτης ζήτησης, τους υποσταθμούς και τις γραμμές μεταφοράς και διανομής και τους συνδεδεμένους φορείς που επηρεάζονται (μεταξύ άλλων σε διασυνοριακό επίπεδο) σε περίπτωση επιτυχούς κυβερνοεπίθεσης ή κυβερνοπεριστατικού. Τα κράτη μέλη θα πρέπει επίσης να διασφαλίσουν ότι οι διαχειριστές δικτύων ενέργειας διαθέτουν πλαίσιο επικοινωνίας με όλα τα βασικά ενδιαφερόμενα μέρη, για την ανταλλαγή σημάτων έγκαιρης προειδοποίησης και τη συνεργασία στη διαχείριση κρίσεων. Για την ανταλλαγή ευαίσθητων πληροφοριών με όλα τα σχετικά ενδιαφερόμενα μέρη, τις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών και τις αρμόδιες αρχές, θα πρέπει να υπάρχουν δίαυλοι δομημένης επικοινωνίας και να χρησιμοποιούνται συμφωνημένοι μορφότυποι.

8) Ειδικότερα, οι φορείς εκμετάλλευσης δικτύων ενέργειας θα πρέπει:

α) να εξασφαλίζουν ότι οι νέες συσκευές, συμπεριλαμβανομένων των συσκευών του Διαδικτύου των Πραγμάτων, έχουν και θα διατηρούν επίπεδο κυβερνοασφάλειας κατάλληλο για την κρισιμότητα της κατάστασης σε κάθε τοποθεσία·

β) να εξετάζουν επαρκώς τις κυβερνο-υλικές επιπτώσεις κατά την εκπόνηση και την τακτική αναθεώρηση των σχεδίων επιχειρησιακής συνέχειας·

γ) να θεσπίσουν κριτήρια σχεδιασμού και αρχιτεκτονική που θα εξασφαλίζουν την ανθεκτικότητα του δικτύου, η οποία θα μπορούσε να επιτευχθεί με:

— την εφαρμογή λεπτομερών μέτρων άμυνας ανά τοποθεσία, ειδικά προσαρμοσμένων στην κρισιμότητα της κατάστασης της τοποθεσίας·

— τον εντοπισμό των κόμβων κρίσιμης σημασίας, τόσο από άποψη ικανότητας ηλεκτροπαραγωγής όσο και από άποψη αντικτύπου στους πελάτες· οι κρίσιμες λειτουργίες ενός δικτύου θα πρέπει να σχεδιάζονται κατά τρόπον ώστε να μετριάζεται ο κίνδυνος που μπορεί να προκαλέσει αλυσιδωτές επιπτώσεις, λαμβάνοντας υπόψη τις εφεδρείες, την ανθεκτικότητα στις ταλαντώσεις φάσης και τα μέτρα προστασίας έναντι της αλυσιδωτής αποκοπής φορτίου·

— τη συνεργασία με άλλους σχετικούς φορείς και με τους προμηθευτές τεχνολογίας για την πρόληψη των αλυσιδωτών επιπτώσεων, διά της εφαρμογής κατάλληλων μέτρων και υπηρεσιών·

— τον σχεδιασμό και την κατασκευή δικτύων επικοινωνίας και ελέγχου με σκοπό τον περιορισμό των επιπτώσεων τυχόν υλικής και λογικής αστοχίας σε περιορισμένα τμήματα των δικτύων και τη διασφάλιση κατάλληλων και ταχέων μέτρων μετριασμού.

ΚΛΗΡΟΔΟΤΗΜΕΝΗ ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ ΑΙΧΜΗΣ

9) Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα σχετικά ενδιαφερόμενα μέρη, ιδίως οι διαχειριστές δικτύων ενέργειας και οι πάροχοι τεχνολογίας, ιδιαιτέρως δε οι φορείς εκμετάλλευσης βασικών υπηρεσιών που προσδιορίζονται βάσει της οδηγίας NIS, εφαρμόζουν τα σχετικά μέτρα ετοιμότητας στον τομέα της κυβερνοασφάλειας που σχετίζονται με τον συνδυασμό της κληροδοτημένης τεχνολογίας με την τεχνολογία αιχμής στον τομέα της ενέργειας. Πράγματι, στο υφιστάμενο ενεργειακό σύστημα συνυπάρχουν δύο διαφορετικοί τύποι τεχνολογιών: μια παλαιότερη τεχνολογία με διάρκεια ζωής από 30 έως 60 έτη, που είχε σχεδιαστεί πριν από την εποχή της κυβερνοασφάλειας, και σύγχρονος εξοπλισμός, κατάλληλος για την υπερσύγχρονη ψηφιοποίηση και τις έξυπνες συσκευές.

10) Κατά την εφαρμογή της παρούσας σύστασης, τα κράτη μέλη θα πρέπει να ενθαρρύνουν τους διαχειριστές δικτύων ενέργειας και τους προμηθευτές τεχνολογίας να συμμορφώνονται με τα σχετικά διεθνώς αποδεκτά πρότυπα κυβερνοασφάλειας, όπου αυτό είναι δυνατόν. Εντωμεταξύ, κατά τη σύνδεση συσκευών με το ηλεκτρικό δίκτυο τα ενδιαφερόμενα μέρη και οι πελάτες θα πρέπει να υιοθετούν μια προσέγγιση προσανατολισμένη στην κυβερνοασφάλεια.

11) Ειδικότερα, οι προμηθευτές τεχνολογίας θα πρέπει να παρέχουν δοκιμασμένες λύσεις για ζητήματα ασφαλείας σε κληροδοτημένες τεχνολογίες και σε τεχνολογίες αιχμής. Οι λύσεις αυτές θα πρέπει να παρέχονται δωρεάν και αμέσως μόλις καταστεί γνωστό οποιοδήποτε σχετικό ζήτημα ασφάλειας.

12) Ειδικότερα, οι διαχειριστές δικτύων ενέργειας θα πρέπει:

α) να αναλύουν τους κινδύνους που προκύπτουν από τη σύνδεση κληροδοτημένων προσεγγίσεων με προσεγγίσεις του Διαδικτύου των Πραγμάτων και να έχουν επίγνωση των εσωτερικών και εξωτερικών διεπαφών και των τρωτών τους σημείων·

β) να λαμβάνουν τα κατάλληλα μέτρα κατά των κακόβουλων επιθέσεων που προέρχονται από μεγάλο αριθμό καταναλωτικών συσκευών ή εφαρμογών που ελέγχονται με κακές προθέσεις·

γ) να δημιουργήσουν αυτοματοποιημένο σύστημα παρακολούθησης και ανάλυσης συμβάντων που σχετίζονται με την ασφάλεια σε κληροδοτημένα περιβάλλοντα και σε περιβάλλοντα του Διαδικτύου των Πραγμάτων, όπως ανεπιτυχείς απόπειρες σύνδεσης, συναγερμούς θυρών για το άνοιγμα ερμαρίων ή άλλα συμβάντα.

δ) να διενεργούν σε τακτική βάση ειδική ανάλυση επικινδυνότητας για την κυβερνοασφάλεια σε όλες τις κληροδοτημένες εγκαταστάσεις, ιδίως κατά τη σύνδεση παλαιών με νέες τεχνολογίες· δεδομένου ότι οι κληροδοτημένες εγκαταστάσεις αντιπροσωπεύουν συχνά πολύ μεγάλο αριθμό περιουσιακών στοιχείων, η ανάλυση επικινδυνότητας μπορεί να πραγματοποιηθεί ξεχωριστά ανά κατηγορία περιουσιακού στοιχείου·

ε) να ενημερώνουν το λογισμικό και το υλισμικό των κληροδοτημένων συστημάτων και των συστημάτων του Διαδικτύου των Πραγμάτων, χρησιμοποιώντας την πλέον πρόσφατη έκδοση όπου ενδείκνυται· παράλληλα, οι διαχειριστές των δικτύων ενέργειας θα πρέπει να εξετάζουν το ενδεχόμενο λήψης συμπληρωματικών μέτρων, όπως η κατάτμηση του συστήματος ή η προσθήκη εξωτερικών φραγμών ασφάλειας, όταν η χρήση τοπικών προσθηκών ασφαλείας ή η ενημέρωση θα ήταν επαρκής αλλά δεν είναι δυνατή, για παράδειγμα για μη υποστηριζόμενα προϊόντα·

στ) να συντάσσουν τις προσκλήσεις υποβολής προσφορών λαμβάνοντας υπόψη την κυβερνοασφάλεια, δηλαδή να ζητούν πληροφορίες σχετικά με τα χαρακτηριστικά ασφάλειας, να απαιτούν τη συμμόρφωση με τα υφιστάμενα πρότυπα κυβερνοασφάλειας, να διασφαλίζουν τη συνεχή υποβολή προτάσεων συνέγερσης, χρήσης τοπικών προσθηκών ασφαλείας και μετριασμού σε περίπτωση εντοπισμού τρωτών σημείων, και να αποσαφηνίζουν την ευθύνη του πωλητή σε περίπτωση κυβερνοεπιθέσεων ή κυβερνοπεριστατικών·

ζ) να συνεργάζονται με τους προμηθευτές τεχνολογίας για την αντικατάσταση των κληροδοτημένων συστημάτων, όποτε αυτό είναι επωφελές για λόγους ασφάλειας, αλλά λαμβανομένων υπόψη κρίσιμων λειτουργιών του συστήματος.

ΠΑΡΑΚΟΛΟΥΘΗΣΗ

13) Τα κράτη μέλη θα πρέπει να κοινοποιούν στην Επιτροπή, εντός 12 μηνών από την έκδοση της παρούσας σύστασης, και ανά διετία στη συνέχεια, λεπτομερείς πληροφορίες σχετικά με την κατάσταση εφαρμογής της παρούσας σύστασης μέσω της ομάδας συνεργασίας NIS.

ΕΠΑΝΕΞΕΤΑΣΗ

14) Βάσει των πληροφοριών που υποβάλλονται από τα κράτη μέλη, η Επιτροπή θα επανεξετάσει την εφαρμογή της παρούσας σύστασης και θα αξιολογήσει κατά πόσον απαιτούνται περαιτέρω μέτρα, όπως ενδείκνυται, σε διαβούλευση με τα κράτη μέλη και τους σχετικούς ενδιαφερόμενους φορείς.

ΑΠΟΔΕΚΤΕΣ

15) Η παρούσα σύσταση απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 3 Απριλίου 2019.

Για την Επιτροπή
Miguel ARIAS CAÑETE
Μέλος της Επιτροπής