

מצב אבטחת הסייבר של ישראל חמור מכפי שנדמה,
אך יש עוד מה לעשות...
ישראל נחשבת למעצמת סייבר, אך בעיקר בתחום ההתקפי ופחות בהגנתי. הפער בין כמות הסטארט-אפים בתחום אבטחת המידע לבין העלייה המטאורית בכמות המתקפות המוצלחות על המשק הישראלי ממחיש זאת יותר מכל. אז מהם האתגרים בתחום אבטחת הסייבר ומה צריך לעשות כדי להתמודד מולם?

Commend הפכה את אבטחת ה-IT בכלל ואת אבטחת הסייבר בפרט בראש סדר העדיפויות.

**כריזה ואינטרקום IP עם תקני ISO לאבטחת מידע ברשת
מצורפים תעודות הסמכה:
Certificate-EN-ISO-27001-EN-2013
IEC62443-4-1-Certificate-Commend-1221**

הגנה ואבטחת נתוני לקוחות חיוניים כדי לזכות באמון המשתמשים שלנו,
מכיוון שהריבוי ההולך וגדל של תהליכים דיגיטליים חדשים בתחום הטכנולוגי, באופן טבעי נושא זה מהווה פתח להתקפה הולכת וגדלה לפושעי סייבר, תוכנות זדוניות, הונאת נתונים והתחזות לסיסמאות או אישורי גישה. נושאים אלו הינם רק חלק קטן מהאיומים שמשתמשים צריכים להיות מוגנים מפניהם.

אבטחת מערכת Commend של היום מושרשת היטב ב-50 שנות ניסיון בתכנון ושכלול טכנולוגיית אבטחת אינטרקום כריזה ותקשורת.

אבטחה והגנה על נתונים נטועות באמון. אנשים יקבלו וישתמשו בפתרונות ובשירותים רק אם הם אמינים.

כדי להדוף התקפות אפשריות,
Commend הפכה את אבטחת ה-IT בכלל ואת אבטחת הסייבר בפרט בראש סדר העדיפויות.
אנו, חברת סברלופון, מודעים לחלוטין לאחריותנו המכרעת בכל הנוגע לבטיחות ומהימנות של פתרונות האבטחה והתקשורת המקצועיים שלנו. כתוצאה מכך, אנו תמיד משתדלים לתקשר ולהפגין את המחויבות שלנו כמובילת שוק מהימנה לקידום הידע הקולקטיבי והניסיון המשותף שלנו.

מסיבה זו, אנו מפתחים את הפתרונות שלנו מתוך מחשבה על אבטחה והגנה על נתונים, על מנת להבטיח את **ההגנה הטובה ביותר על הנתונים והתשתיות של לקוחותינו.**

מתכנון המוצר הראשוני ועד להטמעתו ולשירות לאחר המכירה, 'פרטיות ואבטחה לפי עיצוב' היא העיקרון המנחה וההבטחה המוצקה ללקוחותינו שכל תכונה ופונקציה של מוצר נבחנת מולה.



עם עליית פשעי הסייבר, חברתינו דוגלת בהקשחת המערכת וההגנה על פתרונות Commend מקומיים ושירותי Symphony Commend מקוריים בענן מפני פריצות אבטחה.

נושא זה **נמצא בחזית תהליך פיתוח המוצר שלנו**. בהתקנות סופיות באתר הלקוח, גישת "פרטיות ואבטחה לפי עיצוב" שלנו משתרעת על שילוב של אמצעים בארבע שכבות בסיסיות:

אבטחה פיזית – אבטחה זו מספקת הגנה פיזית לרכיבים רגישים לאבטחה כגון יחידות קצה, קריאת דלת ברשת וכדומה.

האמצעים שננקטו למטרה זו כוללים מחברי IP Commend **Secure** המנתקים את חיבור הרשת במקרה של **חבלה במכשיר כדי להדוף ניסיונות פריצה**.

אבטחת רשת – אבטחה זו מבטיחה חיבורי רשת מאובטחים של רכיבים מקומיים, כמו גם שירותים מבוססי אינטרנט ושירותי ענן של מערכת סימפוניה.

גישה מבוקרת אבטחה לתשתיות רשת הולכת "יד ביד" עם אמצעי אבטחת מידע (כגון הצפנה מנקודה לנקודה) בהתאם לנורמות ותקנים מוכחים.

בדיוק מהסיבה הזו פותחה מההתחלה פלטפורמת Symphony Commend, תוצר " הענן " בנוי בצורה של "אבטחה משלב עיצוב המוצר " בהתאם לגישת הפרטיות והאבטחה של Commend (PSBD). בהתאם למחויבות זו, Commend הטמיעה גם מערכת ניהול אבטחת מידע (ISMS) תואמת IEC/ISO 27001:2013 כדי לשמור על בטיחות כל הנתונים הארגוניים כמו גם מידע על לקוחות וספקים.

בטיחות כשלים - אמצעים שונים, החל מעדכונים אוטומטיים ועד לאסטרטגיות כשל מקוריות בענן משמשות כדי להבטיח זמינות ללא הפרעה של מערכות ושירותי Commend, גם במקרה של כשל בחיבור לרשת.

כתוצאה מכך, אבטחת סייבר מרובת רמות מאפשרת למשתמשים ליהנות מביצועי שירות סברלופון / Commend, ברמה הגבוהה ביותר.

מידע נוסף האתר:
www.commend.com

