SANS SECURITY AWARENESS

מדריך יישום מודעות אבטחה –
עבודה מאובטחת בבית

תקציר מנהלים

בשל וירוס הקורונה, ארגונים רבים נאלצים להדריך את העובדים שלהם לעבוד מהבית. הדבר עשוי להוות אתגר לארגונים רבים שבהם אין את המדיניות, הטכנולוגיה וההדרכות הנוגעות לאבטחת צוותי עבודה העובדים מרחוק. בנוסף, ישנם עובדים רבים שייתכן ואינם מכירים או אינם חשים בנוח עם הרעיון של עבודה מהבית. המטרה של מדריך זה היא לאפשר לכם לספק הדרכה מהירה לאותם אנשים כך שיהיו מאובטחים במידה הרבה ביותר ככל שניתן. אם יש לכם שאלות כיצד להשתמש במדריך זה, אנא צרו קשר איתנו באמצעות כתובת הדוא"ל support@sans.org.

מכיוון שסביר שהעובדים שלכם עוברים תקופה הכרוכה במתח ושינוי ובנוסף סביר שהארגון שלכם מוגבל בזמן ומשאבים, מדריך אסטרטגי זה מתמקד בגיבוש הדרכה שתהיה פשוטה ככל שניתן. אנו ממליצים להתמקד בסיכונים החשובים ביותר שיש להם את ההשפעה הגדולה ביותר, כפי שאנו מפרטים להלן. חשבו על כך כנקודת פתיחה. אם ישנם סיכונים או נושאים נוספים שתרצו להוסיף, אנא עשו זאת. אבל עליכם להבין שככל שתעמיסו על העובדים שלכם יותר התנהגויות, תהליכים או טכנולוגיות, תפחת הסבירות שהם יוכלו ליישם את כולם.

כיצד להשתמש במדריך זה

אנו ממליצים להתחיל בקריאת החומר המובא במדריך זה וסקירת הקישורים לחומרים השונים המסופקים על מנת שתקבלו מושג מה זמין עבורכם. תוכלו להבחין שעבור כל סיכון אנו מספקים מגוון חומרים שונים בהם תוכלו להשתמש כדי לשתף ולהדריך את הארגון שלכם. מגוון זה מאפשר לכם לבחור את המודליות שלדעתכם תתאים באופן היעיל ביותר לצרכים ולתרבות שלכם. לאחר שסיימתם לקרוא מסמך זה, קראו את שני המסמכים הנלווים תבנית התקשורת (Communications Template) וגליון עובדות (Factsheet) המסופקים בערכה זו על מנת להבין טוב יותר מה אתם מנסים להשיג. לאחר שבחנתם את התיעוד, עליכם לתאם עם שתי קבוצות מפתח.

1. **צוות אבטחה:** עליכם לתאם עם צוות האבטחה שלכם על מנת להבין טוב יותר מהם הסיכונים המרכזיים אותם אתם מנסים לנהל. אנו זיהינו במסמך זה את הסיכונים שאנו חושבים שהם הסיכונים החשובים והנפוצים ביותר עבור צוות עבודה העובד מהבית אבל ייתכן והסיכונים שלכם הינם שונים. הערת אזהרה, שגיאה נפוצה אותה צוותי אבטחה עושים היא לנסות לנהל את כל הסיכונים ולהעמיס על האנשים מספר רב של מדיניות ודרישות. נסו להגביל את מספר הסיכונים אליהם תתייחסו ככל הניתן. לאחר שזיהיתם ותיעדפתם את הסיכונים, וודאו מהן ההתנהגויות שינהלו סיכונים אלה. כפי שצויין, במידה ולארגון שלכם אין את הזמן או המשאבים לכך, עשו שימוש במה שתיעדנו להלן.
2. **תקשורת:** לאחר שזיהיתם מהם הסיכונים האנושיים החשובים ביותר מבחינתכם ומהן ההתנהגויות המרכזיות לניהול סיכונים אלה, שתפו פעולה עם צוות התקשורת שלכם כדי לשתף ולהדריך את העובדים שלכם בנוגע להתנהגויות אלה. לתכניות מודעות האבטחה הטובות ביותר יש שותפויות חזקות עם צוות התקשורת שלהם. במידת האפשר, בדקו האם אתם יכולים לשבץ חבר צוות תקשורת בצוות האבטחה שלכם. כאשר אתם מתקשרים העובדים שלכם, אחד גורמי המשיכה היעילים בהם תוכלו להשתמש על מנת להביא לשיתוף פעולה מצידם היא להדגיש שהדרכה זו תאבטח אותם במסגרת העבודה ובנוסף תאפשר להם ליצור בית מאובטח ותגן עליהם ועל בני המשפחה שלהם.

בסופו של דבר, באמצעות העבודה עם שני צוותים אלה אתם מנסים להפוך את נושא האבטחה לפשוט ככל האפשר עבור העובדים שלכם ולהניע אותם, שני הגורמים המרכזיים המובילים לשינוי בהתנהגות. אנו מציעים להקים וועדת ייעוץ שתורכב מאנשי מפתח שהמשוב שלהם והנתונים שיספקו יאפשרו להוציא לפועל את התכנית. בנוסף לצוות האבטחה ולצוות התקשורת, ייתכן ותרצו לשתף ולתאם מול מחלקת משאבי אנוש והמחלקה המשפטית.

מארז הורדה דיגיטלית MGT433

SANS Institute מספק את ההדרכה בת היומיים MGT433: כיצד ליצור, לשמר ולמדוד תכנית מודעות אבטחה יעילה. הדרכה אינטנסיבית זאת מספקת את כל התיאוריה, הכישורים, מסגרת העבודה והמשאבים הנחוצים לגיבוש תכנית מודעות יעילה שתאפשר לכם לנהל ולמדוד באופן יעיל את הסיכונים האנושיים עימם אתם מתמודדים. כחלק ממדריך זה אנו מספקים גישה חופשית לחומרים בתוך מארז הורדה דיגיטלית (Digital Download Package) המכיל תבניות ומשאבי תכנון. בעוד שסביר להניח שחומרים אלה הם מעל ומעבר לצרכים של יוזמה זו, חומרים אלה עשויים להיות רבי ערך עבור ארגונים גדולים יותר או לפריסות מורכבות יותר.

תגובה לשאלות עובדים

בנוסף לתקשורת עם צוות העובדים ולהדרכה שלהם, אנו ממליצים מאד לגבש סוג כלשהו של טכנולוגיה או פורום שם תוכלו לתת מענה לשאלות מהאנשים, בעדיפות למענה בזמן אמת. זה יכול לכלול כתובת מייל, סקייפ או ערוץ צ'אט Slack ייעודיים, או סוג כלשהו של פורום מקוון כדוגמת Yammer. רעיון אחר הוא ליצור שידור אינטרנט בנושא אבטחה שישודר מספר פעמים במשך השבוע כך שאנשים יוכלו לבחור את הזמן המתאים להם ולהשתתף בשידור החי ואולי אף לשאול שאלות. המטרה היא להפוך את נושא האבטחה לנגיש ככל הניתן ולסייע לאנשים במענה לשאלות שלהם. זוהי הזדמנות מצוינת לשתף את העובדים שלכם ולהעניק לתחום האבטחה פנים ידידותיות, נסו לנצל הזדמנות זו. זכרו, על מנת להיות יעילים עליכם להקדיש משאבים לתווך את כל ערוצי האבטחה ולהגיב באופן פעיל לשאלות.

סיכונים וחומרי הדרכה

אנחנו זיהינו שלושה סיכוני ליבה שעליכם לנהל עבור העובדים שלכם העובדים מרחוק. אלו מהווים את נקודת הפתיחה והם ככל הנראה אלו שיהיו בעלי הערך הרב ביותר עבורכם. לכל סיכון המופיע למטה יש קישורים למספר משאבים שיסייעו להעביר את הנושא ולהדריך בנוגע אליו. אנו מספקים חומרי תקשורת רבים כך שתוכלו לבחור את אלו שלהם תהיה ההשפעה הרבה ביותר על התרבות שלכם. בנוסף, כמעט כל החומרים מגיעים במספר שפות. במידה והדבר מעמיס עליכם יתר על המידה והזמן שלכם מאד מוגבל, אז אנחנו ממליצים שפשוט תתקדמו עם שני החומרים המפורטים להלן.

1. דף העובדות של עבודה מאובטחת מהבית (כלול בערכת היישום שלכם).
2. סרטון יצירת בית מאובטח (באנגלית) הסרטון זמין גם בשפות אחרות כאן

הנדסה חברתית

אחד הסיכונים הגדולים ביותר עימם אלו שעובדים מרחוק יצטרכו להתמודד, בייחוד בתקופה זו של שינוי דרמטי וסביבה מלאת תחושת דחיפות, הוא הסיכון של התקפות הנדסה חברתית. הנדסה חברתית היא התקפה פסיכולוגית במסגרתה התוקפים עובדים על הקורבנות שלהם או מרמים אותם וגורמים להם לעשות שגיאה, מה שיהיה קל יותר לעשות בזמן של שינוי ובלבול. המפתח הוא להדריך את האנשים להבין מהי הנדסה חברתית, כיצד לאתר את הסימנים הנפוצים ביותר של התקפת הנדסה חברתית ומה לעשות לאחר שהבחינו בהם. תוודאו שאינכם מתמקדים בהתקפות דיוג באמצעות דוא"ל בלבד, ושאתם מתייחסים גם לשיטות אחרות הכוללות שיחות טלפון, שליחת הודעות, התקשרות באמצעות רשת חברתית או חדשות מזויפות. תוכלו למצוא את החומרים הדרושים לכם כדי להדריך ולחזק נושא זה בספריית חומרי עזר בנושא הנדסה חברתית (Social Engineering Support Materials) שלנו. בנוסף קישורים לשני סרטוני הדרכת מודעות של SANS, אליהם תוכלו לגשת וגם אלו מסופקים במספר שפות.

- הנדסה חברתית (אנגלית) זמין גם בשפות אחרות כאן
- דיוג (אנגלית) זמין גם בשפות אחרות כאן

סיסמאות חזקות

כפי שמפורט ב- Verizon DBIR השנתי, סיסמאות חלשות ממשיכות להיות אחד מהגורמים העיקריים לפריצות בקנה מידה גלובלי. יש ארבע התנהגויות מרכזיות שיסייעו לנהל סיכון זה, כמפורט להלן. תוכלו למצוא את החומרים הנדרשים לכם כדי להדריך ולחזק תחום זה ואת ארבעת ההתנהגויות המרכזיות הללו בספריית סיסמאות (Passwords) שלנו.

- ביטויי סיסמה (שימו לב שגם מורכבות סיסמה וגם תוקף סיסמה אינן).
- סיסמאות ייחודיות עבור כל אחד מהחשבונות
- מנהלי סיסמאות
- MFA (אימות מרובה גורמים). המכונה לעיתים אימות דו-גורמי או אימות דו-שלבי

עדכוני מערכת

הסיכון השלישי הוא להבטיח שכל טכנולוגיה בה חברי הצוות שלכם משתמשים פועלת בגרסה העדכנית ביותר של מערכת ההפעלה, היישומים והיישומים הניידים. עבור אנשים המשתמשים במכשירים פרטיים ייתכן הדבר יצריך הפעלת אפשרות עדכון אוטומטי. תוכלו למצוא את החומרים הנדרשים לכם כדי להדריך ולחזק תחום זה ואת ארבעת ההתנהגויות המרכזיות הללו בספריות תוכנות זדוניות או יצירת בית מאובטח שלנו.

נושאים נוספים שיש להביא בחשבון

- **Wi-Fi**: אבטחת נקודת הגישה שלכם ל- Wi-Fi. נושא זה מכוסה בתוך חומרי יצירת בית מאובטח (Creating a Cybersecure Home). בנוסף, צפו בסרטון זה סרטון יצירת בית מאובטח - Creating a Cybersecure Home Video (באנגלית) הזמין גם בשפות נוספות כאן.

- **VPN's**: מה זה VPN ומדוע עליכם להשתמש ברשת כזו. אנו ממליצים לעיין בעלון OUCH (אוגוסט) בנושא VPNs.

- **עבודה מרחוק:** זה עבור אנשים העובדים מרחוק אבל אינם עובדים מהבית, כגון בבתי קפה, טרמינלים בנמלי תעופה או בתי מלון. שקלו את האפשרות להשתמש בסרטון שלנו סרטון הדרכה עבודה מרחוק (Working Remotely training video) (באנגלית) הזמין גם בשפות אחרות כאן.

- **ילדים / אורחים:** על מנת לחזק את הרעיון שבני משפחה / אורחים אינם יכולים לגשת למכשירים הקשורים לעבודה, שקלו להשתמש בסרטון הדרכת עבודה מרחוק (Working Remotely training video) (באנגלית) הזמין גם בשפות אחרות כאן.

- **איתור / תגובה:** האם אתם רוצים שאנשים ידווחו אם הם חושדים באירוע שהתרחש בזמן שעבדו מהבית? במידה וכן, מה ברצונכם שידווחו ומתי? נושא זה מכוסה בחומרי פריצה שלנו.

עלוניOUCH (אאוץ)

בנוסף, שקלו את האפשרות להשתמש ב- OUCH newsletters (עלוני אאוץ) הזמינים לציבור כדי לתמוך בתכנית שלכם, כל אחד מהעלונים מתורגם ליותר מעשרים שפות. להלן פירוט של עלוני OUCH (אאוץ) שאנו חושבים שמספקים את התמיכה הטובה ביותר ליוזמה שלכם לעבודה מאובטחת מהבית. תוכלו למצוא את כל העלונים באינטרנט OUCH Security Awareness Newsletter Archives (ארכיון עלוני אאוץ למודעות אבטחה).

סקירה

Four Steps to Staying Secure (ארבעה צעדים לשמירה על האבטחה)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (יצירת בית מאובטח)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

הנדסה חברתית

Social Engineering (הנדסה חברתית)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (שליחת הודעות / סמישינג)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (הונאות מותאמות אישית)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (הונאת מנכ"ל)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (התקפות / הונאות באמצעות שיחת טלפון)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (עצרו את הדיוג)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (הונאה דרך מדיה חברתית)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

סיסמאות

Making Passwords Simple (יצירת סיסמאות בקלות)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login - 2FA (נעילת כניסה - 2FA)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

בנוסף

Yes, You Are a Target (כן, אתם המטרה)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (מכשירים חכמים בבית)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

עצות מהירות

עצות וטריקים שתוכלו לשתף בקלות לצריכת הפורמט.

- הצעדים היעילים ביותר בהם תוכלו לנקוט על מנת לאבטח את הרשת האלחוטית בבית שלכם היא לשנות את סיסמת המנהל המגיעה כברירת מחדל, לאפשר הצפנת WPA2 ולהשתמש בסיסמה חזקה לרשת האלחוטית שלכם.
- היו מודעים לכל המכשירים המחוברים לרשת הביתית שלכם, כולל מוניטורים של התינוק, קונסולות משחק, טלוויזיות, מכשירים ביתיים או אפילו הרכב שלכם. וודאו שכל המכשירים הללו מוגנים בעזרת סיסמה חזקה ו/או שהם פועלים על הגרסה העדכנית ביותר של מערכת ההפעלה שלהם.
- אחת הדרכים היעילות ביותר באמצעותה תוכלו להגן על המחשב בבית שלכם היא לוודא שגם מערכת ההפעלה וגם היישומים שלכם מעודכנים ופועלים עם טלאים. יש להפעיל את אפשרות העדכון האוטומטי ככל שניתן.
- בסופו של דבר, שכל ישר והגיון בריא הם ההגנה הטובה ביותר שלכם. אם דואר אלקטרוני, שיחת טלפון או הודעה מקוונת, נראים מוזרים, חשודים או טובים מכדי להיות אמיתיים, זו עשויה להיות התקפה.
- וודאו שלכל אחד מהחשבונות שלכם יש סיסמה נפרדת, ייחודית. לא מצליחים לזכור את כל הסיסמאות / ביטויי הסיסמה שלכם? שקלו להשתמש במנהל סיסמאות כדי לשמור באופן מאובטח את כל הסיסמאות.
- אחת הדרכים הטובות ביותר לאבטח כל חשבון הוא שימוש באימות דו-שלבי. אימות דו-שלבי הוא כאשר אתם נדרשים לתת גם סיסמה וגם קוד הנשלח אליכם או מופק על ידי המכשיר הנייד שלכם. דוגמאות לשירותים התומכים באימות דו-שלבי כוללות את ג'ימייל (Gmail), דרופבוקס (Dropbox) וטוויטר (Twitter).
- דיוג מתרחש כאשר תוקף מנסה לרמות אתכם ולגרום לכם ללחוץ על קישור זדוני או לפתוח קובץ המצורף להודעת דוא"ל .תחשדו בכל דוא"ל או הודעה מקוונת היוצרים תחושת דחיפות ,מכילים שגיאות איות או פונים אליכם בשם "לקוחות יקרים."

מדדים

מדדי התנהגות הינם בעייתיים עבור מצב זה שכן קשה יותר למדוד את אופן ההתנהגות של האנשים בבית. בנוסף, חלק מההתנהגויות הללו אינן ספציפיות לעבודה (למשל אבטחת מכשיר ה- Wi-Fi שלהם). אולם, תוכלו למדוד מעורבות. אנחנו מצאנו שנושאים אישיים או רגשיים כגון אלה יכולים להיות מושכים מאד ולגרום לעניין רב יותר מנושאים אחרים. מכיוון שכך, מדדים כאלה יכולים להיות בעלי ערך רב.

- **אינטראקציה:** באיזו תכיפות אנשים שואלים שאלות, מפרסמים רעיונות או מבקשים עזרה בכל אחד מערוצי האבטחה או הפורומים שאתם מארחים?
- **סימולציות:** ערכו מעין סימולציות של הנדסה חברתית, כגון דיוג או התקפות מבוססות הודעות או שיחות טלפון.

לרשימת מדדים מקיפה יותר, הורידו את מדד מודעות האבטחה האינטראקטיבי (Security Awareness Metrics Matrix) מתוך המארז להורדה דיגיטלית MGT433.

רישיון

מחבר ערכת היישום

ללאנס שפיצנר (Lance Spitzner) מעל 20 שנות ניסיון אבטחה בחקר איומי סייבר, ארכיטקטורת אבטחה, מודעות והדרכה. הוא היה בין החלוצים בתחומי ההונאה ומודיעין הסייבר עם יצירת מלכודות הדבש (honeynets) וייסוד Honeynet Project. כמדריך SANS הוא פיתח את הקורסים MGT433: מודעות אבטחה ו- MGT521: תרבות אבטחה. בנוסף, לאנס פרסם שלושה ספרים בתחום האבטחה, ייעץ ביותר מ- 25 מדינות וסייע ליותר מ- 350 ארגונים ליצור תכניות מודעות אבטחה ותרבות אבטחה כדי לנהל את הסיכונים האנושיים שלהם. לאנס מציג באופן קבוע, פעיל סדרתי בטוויטר (@lspitzner) ועובד על מספר פרויקטים של אבטחת קהילה. לפני העיסוק באבטחת מידע, מר שפיצנר שירת כקצין שריון בכוח הפריסה המהיר (Rapid Deployment Force) של הצבא וקיבל את תואר ה- MBA מאוניברסיטת אילינוי

אודות SANS Institute

SANS Institute הוקם בשנת 1989 כארגון שיתופי למחקר והשכלה. מכון SANS הוא הארגון המהימן ביותר והספק הגדול ביותר של הדרכות והסמכות אבטחת סייבר לאנשי מקצוע במוסדות ממשלתיים ומסחריים בכל רחבי העולם. מדריכי SANS הינם ידועים ובעלי שם והדריכו יותר מ- 60 קורסים ביותר מ- 200 אירועים חיים של הדרכת אבטחת סייבר, בנוסף להדרכות מקוונות. GIAC, סניף של SANS Institute, מתקף את ההסמכות של אנשי ביצוע ביותר מ- 35 אישורים באבטחת סייבר יישומיים וטכניים. SANS Technology Institute, חברת בת עצמאית בעלת הכרה אזורית, מציע לימודי תואר שני באבטחת סייבר. SANS מציעה מספר עצום של משאבים בחינם לקהילת אבטחת המידע, כולל פרויקטי קונצנזוס, דו"חות מחקר ועלונים; היא גם מפעילה את מערכת ההתרעה המוקדמת של האינטרנט--Internet Storm Center. במרכז SANS מצויים מספר רב של אנשי מקצוע בתחום האבטחה, המייצגים מגוון ארגונים גלובליים, החל מתאגידים וכלה באוניברסיטאות, העובדים יחד כדי לסייע לכלל קהילת אבטחת המידע.

(https://www.sans.org)