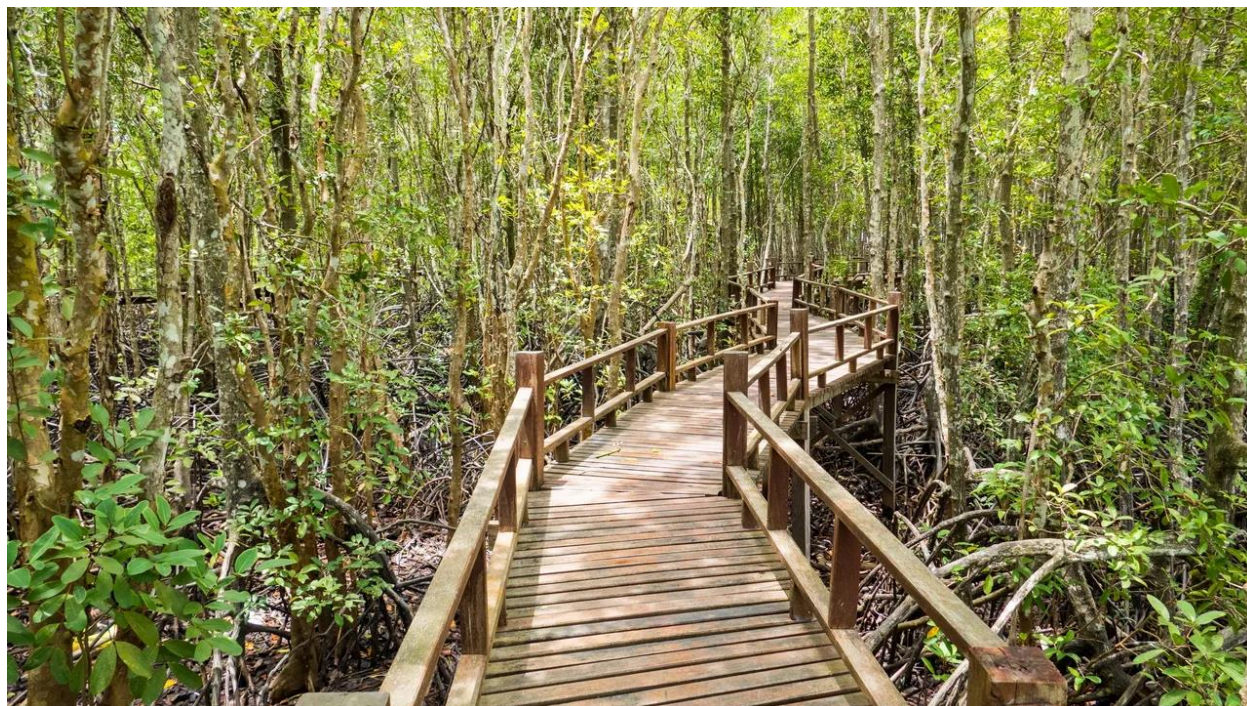


הישרדות בג'ונגל האינטרנט: אתגר לעסקים

[מבוא ENGLISH ARTICLE](#)

אבטחת סייבר והישרדות בג'ונגל אולי נראים רחוקים זה מזה, אבל למעשה יש ביניהם הרבה מן המשותף. בשני המקרים מדובר בהתמודדות עם אימים פוטנציאליים, הסתגלות לסביבה עוינת והגנה על עצמך מפני פגיעה. במאמר זה, נבחן כיצד לשרוד בסביבה דיגיטלית עוינת.



בהקשר של אבטחת סייבר, ישנם שני מושגים נפרדים אך משלימים: תאימות וחוסן.

תאימות

תאימות פירושה הקפדה על מערכת כללים או תקנים שנועדו להפחית את הסיכון להתקפות סייבר ולהגן על נתונים ומערכות. דרישות תאימות יכולות להיות מוטלות על ידי רשויות רגולטוריות, גופי הסמכה או לקוחות. תאימות נתפסת לעתים קרובות כאילוץ או מחויבות, אך היא יכולה גם להביא יתרונות, כגון אמון, מוניטין או תחרותיות. עם זאת, תאימות אינה ערובה לאבטחה מוחלטת, מכיוון שהיא אינה מכסה את כל התרחישים האפשריים וניתן לעקוף אותה על ידי אימים המתפתחים במהירות.

חברות רבות חיפשו והשיגו תאימות, בעיקר באמצעות עמידה בדרישות חוקיות ורגולטוריות מקומיות כמו חוק הגנת הפרטיות, תקנות המפקח על הבנק, תקנות המפקח על שוק ההון, וכן אימוץ תקנים, חוקים ומסגרות עבודה בינלאומיים כמו GDPR, NIST, ISO27001, SOX ועוד. עם זאת, חשוב לציין כי במבדק תאימות לא בוחנים את איכות העמידה, אלא את עצם העמידה, מה שיכול להביא לפער משמעותי בין העובדה שהארגון עומד בכל הדרישות שחלות עליו, אולם רמת העמידות שלו מפני מתקפות סייבר, וכן רמת החוסן שלו להתמודדות עם אירועי סייבר מוגבלות.

חוסן סייבר

חוסן סייבר, מתמקד לא רק בהפחתת הסיכוי למתקפת סייבר, אלא בבניית היכולת והאמצעים להתמודד עם מתקפת סייבר, להגביל את השפעתה ולחזור לפעול במהירות האפשרית. חוסן פירושו להתכונן לבלתי צפוי, לזהות תקריות, להגיב ביעילות וללמוד מניסיון העבר. חוסן נתפס לרוב כנכס או הזדמנות, אך הוא יכול לגרור גם עלויות, מאמץ או סיכונים. חוסן גם הוא אינו ערובה מוחלטת לאבטחה, שכן הוא אינו מונע לחלוטין התקפות סייבר, אך בניית חוסן סייבר מספק, מפחית את ההשפעה הפוטנציאלית של אירוע סייבר, ומאפשר לארגון להמשיך ולפעול גם תחת מתקפה.

אימוץ שני הרבדים של תאימות וחוסן, הכרחי ומשלים כדי לשרוד ב"ג'ונגל האינטרנט", וחברות צריכות למצוא את האיזון הנכון בין השניים, בהתאם להקשר ולמטרות שלהן.

בין אבטחת סייבר והישרדות בג'ונגל יש כמה הבדלים בולטים:

- מידת החשיפה והפגיעות: בג'ונגל הסכנה מיידית וגלויה יותר וההשלכות עלולות להיות קטלניות. במרחב הווירטואלי, **הסכנה מפוזרת ודיסקרטית יותר**, וההשלכות עלולות להתעכב ומגוונות יותר.
- סוג המשאבים והתמיכה הזמינים: בג'ונגל, אתה צריך לסמוך על המשאבים שלך ועל הטבע כדי לשרוד. במרחב הווירטואלי, קיימות רשתות ומערכות בטיחות, הן טכניות והן אנושיות, שיכולות לעזור לך להגן ולהתאושש. **עזרה הדדית היא המפתח להישרדות.**
- רמת השליטה והחופש: בג'ונגל, עליך לציית לחוקי הטבע ולמנהגים המקומיים. במרחב הווירטואלי יש נורמות ותקנות, אבל גם הזדמנויות לעקוף או לחרוג מהם: **אין גבולות באינטרנט, ולוקח פחות משנייה להגיע לכל מחשב על פני כדור הארץ המחובר לאינטרנט!**

אולם למרות ההבדלים בין הישרדות בג'ונגל לחוסן במרחב הווירטואלי, הקווים המקבילים הבאים, יכולים לסייע בבניית העמידות הכוללת בסייבר:

צמצום משטח התקיפה

בראש ובראשונה, עלינו להעריך האם משטח התקיפה שלנו יכול לחשוף אותנו בקלות להתקפות, ועלינו לשאוף לצמצם אותו ככל האפשר, לעשות זאת "חלק" ככל האפשר עבור התוקפים, שסורקים כל כתובת IP בכל האינטרנט בכל יום, מחפשים נקודות תורפה חדשות. אנחנו לא צריכים להיות הכי מהירים בג'ונגל, אנחנו צריכים להיות יותר מהירים ממי שרץ לידינו. תוקפים מעדיפים מטרות קלות, ואנחנו לא רוצים להיות המטרה הזו.



התקפה קלה, עם כל הפגיעויות האלה שמקלות על האקרים להיצמד. תמונה. (Le Dauphiné Libéré).



תקיפה אפשרית, אבל הרבה יותר קשה לאחר שהחולשות נסגרו.

משמעות הדבר היא הגבלת החשיפה של מערכות IT לאיומים פוטנציאליים, על ידי צמצום מספר נקודות הגישה, השירותים והפונקציונליות המיותרים או הפגיעים. **ניהול משטח ההתקפה** כרוך במעקב מתמיד אחר פגמי האבטחה ותיקונם המהיר, כמו גם הערכה שוטפת של סיכונים ואמצעי הגנה.

- שימו בפרוטוקולי הצפנה חלשים לדוגמה, חושף את הארגון לדליפה, מניפולציה או חסימה של תעבורה. לכן חיוני לבחור בפרוטוקולי הצפנה חזקים ועדכניים העומדים בסטנדרטים ובשיטות עבודה מומלצות בינלאומיות.

- עיכוב בעדכון **תיקוני אבטחה** חושף את מערכות המחשוב של החברה למתקפות המנצלות נקודות תורפה ללא תיקון. להיעדר תיקוני אבטחה עלולות להיות השלכות חמורות, כגון השתלטות מרחוק, גניבת זהות, תוכנות כופר או פגיעה בשירות. לכן חיוני ליישם מדיניות של עדכוני תוכנה ומערכת הפעלה קבועים ואוטומטיים.

- **חולשות תוכנה** נגרמות בשל שגיאות בתכנון, בפיתוח או בתצורה של אפליקציות אינטרנט או ניידות, מה שמספק לתוקפים הזדמנויות לפריצה או חטיפה. פרצות יישומים עלולות להוביל לחשיפה, שינוי או מחיקה של נתונים, כמו גם להפצה של תוכנות זדוניות או קוד זדוני. לכן, חיוני לעמוד בתקני איכות ואבטחה של יישומים, ולבדוק אותם באופן קבוע, במיוחד במצבים אמיתיים, תוך שימוש בטכניקות כמו "**צוות אדום**" או "**באג באונטי**".

שמור על האש בוערת!



בואו נסתכל על חמשת המרכיבים הללו שיאפשרו לנו להיות גמישים, "לשמור על האש", מול התקפות סייבר, ושיש להתייחס אליהם, לדעתי, כעדיפות עליונה:



5 actions de "cyber survie" immédiates



1-Chiffrement des disques durs et virtualisation des serveurs

Pour éviter les malicieux *KON Boot* et les *C&C de rançongiciels* :

- **Chiffrement des disques**, SecureBoot activé, virtualisation activée, autorisation d'accès par contrôleur de domaine.
- Correctifs de sécurité et pas de système obsolète (O.S. et navigateurs)

2-Protection des courriels

Pour empêcher les faux courriels de phishing vecteur des rançongiciels:

- Protection des domaines d'émission: SPF – DMARC
- 2FA

3-Mise en œuvre de l'authentification double facteur (2FA)

Pour éviter l'utilisation de fuites de mots de passe :



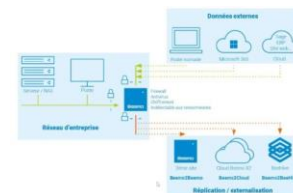
5-Anti-rançongiciel (XDR) Supervision Alertes Remédiation par SOC 24/7/365



4-Mise en place d'une sauvegarde « immuable »

Pour répartir rapidement en cas de cyber - attaque: **Stratégie de sauvegarde 1-2-3**

- 1 Données primaires - 2 Sauvegarde locale
- 3 Sauvegarde hors site
- Sauvegardes chiffrées
- Instantané complet des VM
- Essais de restauration / Plan de secours



1. **הצפנת דיסק ווירטואליזציה של שרת.** טכניקות אלו מגנות על נתונים רגישים המאוחסנים במכונות פיזיות או וירטואליות מפני גניבה, שחיתות או הרס. ההצפנה הופכת את הנתונים לבלתי קריאים ללא מפתח סודי, בעוד וירטואליזציה יוצרת עותקים מבודדים של שרתים שניתן לשחזר במקרה של בעיה.
2. **טלאים (תיקוני אבטחה).** אלו הם עדכוני תוכנה שמתקנים ליקויי אבטחה שזוהו במערכות הפעלה, יישומים או קושחה. תיקונים חיוניים למניעת התקפות הזרקת קוד זדוניות, התקפות מניעת שירות וגניבת זהות. יש ליישם אותם בהקדם האפשרי ולבדוק תאימות לרכיבי מערכת אחרים.
3. **הגנת דואר אלקטרוני.** זה כרוך בסינון של הודעות לא רצויות, הונאה או זדוניות, שעשויות להכיל קבצים מצורפים נגועים, קישורים לאתרים שנפגעו או ניסיונות דיג. הגנת הדואר האלקטרוני כרוכה בשימוש בפתרונות אנטי-ספאם, אנטי-וירוס ואנטי-פישנינג, וכן העלאת מודעות המשתמשים לנוהלי אבטחה טובים (לדוגמה, אי פתיחת הודעות חשודות או בדיקת השולח לפני לחיצה על קישור).
4. **יישום אימות דו-שלבי.** משמעות הדבר היא חיזוק האבטחה בעת גישה לחשבונות מקוונים או משאבים רגישים, על ידי דרישת שני רכיבי זיהוי במקום אחד בלבד. למשל, סיסמה וקוד שנשלחו ב-SMS או סיסמה זמנית וטביעת אצבע. אימות דו-גורמי מפחית את הסיכון לפריצה לחשבון במקרה של גניבה, אובדן או סיסמאות בסיכון.
5. **הטמעת גיבוי בלתי ניתן לשינוי, עם אנטי כופר, (XDR) פיקוח ותיקון על ידי SOC 24/7/365** המטרה היא להגן על נתונים מפני תוכנות כופר, תוכנות זדוניות שחוסמות גישה לקבצים ודורשות כופר כדי לשחרר אותם. גיבוי בלתי ניתן לשינוי כולל אחסון נתונים על מדיום שלא ניתן לשנות או למחוק, כגון הענן או תיבת NAS הממוקמת באתר אחר. הפתרון נגד תוכנות כופר (XDR) מזהה, חוסם ומסיר תוכנות כופר באמצעות ניתוח מתקדם של התנהגות ואיומים. ה (Security Operations Center) -SOC הוא מרכז ניטור ותגובה לאירועים ביטחוניים, המבטיח התערבות מהירה ויעילה במקרה של תקיפה.

להלן מספר דוגמאות למתקפות סייבר אחרונות הממחישות את חשיבותם של אמצעי האבטחה שהוזכרו:

הגנה על דואר אלקטרוני: באוגוסט 2023, אתר monespaceprime.engie.fr המציע הצעות מחיר לתיקונים בבית, היה קורבן לדליפה מסיבית של נתונים אישיים. יותר מ-110,000 כתובות דואר אלקטרוני נחשפו, יחד עם מידע רגיש כמו מספרי טלפון, כתובות דואר ופרויקטי עבודה. הדלפה זו עלולה להיות מנוצלת על ידי פושעי סייבר כדי לנהל קמפיינים דיגים ממוקדים ולנסות להוציא כסף או מידע מקורבנות. הגנה על דואר אלקטרוני הייתה יכולה להפחית את הסיכון של קבלה או פתיחה של הודעות הונאה.

Le site web monespaceprime.engie.fr géré par un sous-traitant d'Engie a été piraté après exploitation d'une faille de sécurité. Des données personnelles de 110 000 utilisateurs inscrits sont tombés entre les mains de cyberattaquants.



Suite au piratage du site web monespaceprime.engie.fr Engie a informé directement les personnes concernées, porté plainte et procédé à une notification auprès de la Cnil. (crédit : D.R.)

אימות דו-שלבי: במרץ 2021 חשפה חברת ציוד הרשת האמריקאית Ubiquiti כי היא נסחטה בעקבות חדירה למערכות ה-ID-שלה. האקרים קיבלו גישה למאגרי מידע המכילים מידע על לקוחות כמו שמות, כתובות דואר אלקטרוני וסיסמאות. לאחר מכן הם איימו לחשוף את הנתונים האלה אלא אם החברה תשלם כופר. אימות דו-שלבי יכול היה למנוע מההאקרים להיכנס לחשבונות לקוחות או עובדים עם הסיסמאות הגנובות בלבד.

L'enquête sur le vol de données au sein d'Ubiquiti pointe la responsabilité d'un employé. Ce dernier a dérobé des données de l'entreprise, demandé une rançon à son employeur, puis s'est fait passer pour un lanceur d'alerte. Retour sur une histoire atypique qui souligne encore une fois le risque de la menace interne.



L'enquête du FBI et de la justice américaine sur le vol de données chez Ubiquiti détaille les différentes étapes du piratage par le principal accusé. (Crédit Photo: Kalhh)

גיבוי בלתי ניתן לשינוי עם תוכנות נגד כופר (XDR) ניטור ותיקון על ידי: SOC 24/7/365 בספטמבר 2020, בית החולים האוניברסיטאי בדיסלדורף, גרמניה, נכה על ידי מתקפת כופר. האקרים הצפנו כוננים קשיחים של שרתים ודרשו כופר כדי לפתוח אותם. התקיפה שיבשה את פעילות בית החולים, ואילצה אותו לדחות את הניתוחים, להעביר חולים או לסגור את מחלקת המיון שלו. **מטופלת אחת אפילו מתה** כי לא ניתן היה לטפל בה בזמן. גיבוי

נגד תוכנות כופר ללא שינוי (XDR) עם ניטור ותיקון SOC 24/7/365 יכול היה לשחזר את הנתונים מבלי לשלם את הכופר, לזהות ולמגר את תוכנת הכופר ולהגיב במהירות לאירוע.

Attaques inquiétantes

«Les attaques peuvent avoir des effets d'autant plus nuisibles que les pirates sont désormais capables de modifier à distance les dossiers des patients ou encore les dispositifs médicaux», assure Bénédicte Boyer-Bévière, évoquant un essai (fructueux si l'on peut dire) réalisé par des équipes de chercheurs. «Le changement d'un dosage, la disparition d'une donnée essentielle, peuvent être à l'origine de mise en danger criminelle de patients. Une patiente allemande de 78 ans, gravement malade, est décédée en raison de sa prise en charge très très ralentie alors que l'hôpital universitaire de Düsseldorf était paralysé par une attaque dans la nuit du 9 au 10 septembre 2020. C'est le premier exemple d'une personne décédée en Allemagne directement à cause d'une cyberattaque. Enfin, selon une enquête sur la sécurité des appareils des établissements de santé connectés à internet, 24% des hôpitaux avaient un taux de mortalité accru après une cyberattaque».

מסקנה (זמנית)

אנו רואים דוגמאות לכך כל יום. על ידי מתן עדיפות עליונה לאבחן את משטח ההתקפה שלנו וליישם את חמשת מרכיבי הישרדות, **נוכל להכיל את רוב התקפות הסייבר**, או לפחות **לשרוד אותן**, במקום להישאר בסכנה ופחד מתמידים.





Save The Date

09.09
2024

BlackHat Hackers
Online Cyber Event

REGISTER NOW

🕒 16:00-18:30 (CET)

✉ Contact info@presale1.com
for sponsorship options

✍ Please Register Now
to Save Your Place



Mauro Israel

Cybersecurity Expert @BIOOOS Advisory Panelist and Leading
Board Member of Worldwide Advisors @Presale1

מאורו ישראל מומחה באבטחת IS כבר יותר מ-25 שנה, עושה קורסים למודעות אבטחה, כנסים, ייעוץ וביקורת אבטחה. מאורו מנהל +1000 משימות ייעוץ, אבטחה וביקורת, במיוחד עבור מפעלים גרעיניים של EDF, CNES, Ariane Espace, חיל האוויר הצרפתי, Bosch, Peugeot PSA, Alcatel, Ford, Credit Immobilier de France, Institut Curie, Bureau Veritas, Valeo, Societe Generale, SFR, Ferrero, Bank of Africa, BOAD, INPI, Safran, Orpea.

מאורו ישראל, חבר מוביל [במועצת העילית העולמית של Presale1](#) ויקיים [באירוע BlackHat](#) הקרוב בתאריך 09.09.2024 - סדנת "אוטומציה של שיקום - בנושא פגיעויות" – האירוע מתקיים אונליין ואליו נרשמו מעל 800 איש נכון לרגע זה. בין החברות השותפות של Presale1 המשתתפות בחסויות Google, Mandiant, ISC2, סוכנות האיחוד האירופאי לאבטחת סייבר ועוד...

מאת - Mauro ISRAEL מומחה לאבטחת סייבר - חבר מוביל במועצת העילית העולמית של Presale1 - תורגם ונערך על ידי מיי ברוקס קמפלר מרצה ויועצת עולמית מובילה בתחום הסייבר – חברת דירקטוריון ההנהלה ב [Presale1](#)

להרשמה לאירוע המקוון ללא עלות או לפרטים אודות חסויות (כולל חסות דוברות) לחצו [כאן](#)





2K followers
Join Presale1 on LinkedIn

Thank you

Stay Warm and Safe! Follow Presale1! Collect your VIP info security kit now!





Presale1TM

All Your Computer Security Needs in 1