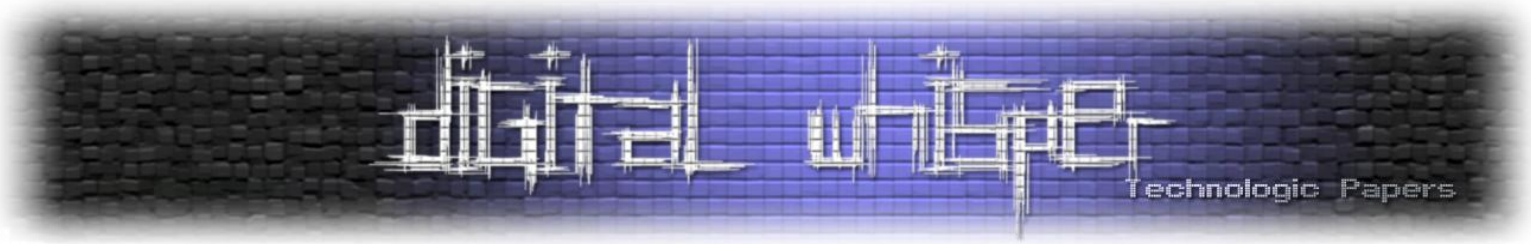


אבטחת מידע בוירטואליזציה

מאת ניר ולטמן

הקדמה

תחום הוירטואליזציה החל לתפוס תאוצה רבה בשנים האחרונות בכלל השווקים , החל מארגונים קטנים וכלה בארגוני ענק. על פי הערכת אנליסטים רבים , המיתון האחרון "עזר" לארגונים רבים לשדרג הרבה מהתשתיות הפיזיות למקבילותיהן הוירטואליות. במאמר זה אסביר על עולם הוירטואליזציה ואסקור את נושא ה-Terminal, אשר ניתן לשלבו יחד עם פתרונות הוירטואליזציה. כמו כן, בסופו של המאמר אפרט על התייחסות אבטחת המידע לנושא הוירטואליזציה.

רקע

בשנות ה-60 משאבי המחשוב היו יקרים מאוד ובעיקר שרתי ה-"Mainframe" של חברת IBM, אשר עד היום משרתים את ליבת הארגונים הגדולים בעולם כמאגר המידע המרכזי. כאמור באותה תקופה החלה חברת IBM לפתח מנגנון אשר יודע לחלק משאבים פיזיים (Hardware Resources) כגון זיכרון ומעבד, למשאבים לוגיים נפרדים אשר עובדים במקביל על אותו שרת פיזי . טכנולוגיה זו נקראת LPAR, כלומר Logical Partition. בשנת 1972 פרסמה חברת IBM את התשתית הוירטואלית שלה על גבי שרתיה , שהחלו משרתי System 370.

פיתוח הטכנולוגיה נזנח בשנות ה- 80 וה-90, כאשר כל מחירי המחשוב בעולם ירדו ובמקביל פותחו אפליקציות רבות מסוג Client-Server אשר חולקות את משאביהן עם תחנות העבודה שבקצה הרשת . החל מסוף שנות ה- 90 הטכנולוגיה תפסה תאוצה והיום וירטואליזציה נחשבת לאחד הנושאים החמים בקרב אנשים טכנולוגיים ואף מנהלי ארגונים.

מה היא וירטואליזציה?

חוק מור שנקבע על ידי גורדון מור (מייסד חברת אינטל) מראה את נכונות הנבואה, בה כל שנה וחצי או שנתיים יוכפל מספר הטרנזיסטורים במעגלים משולבים זולים. חוק זה הוכיח עצמו כבר יותר מ-40 שנה. השערת מומחים רבים הי א שחוק מור יחדל מלהתקיים בעוד מספר שנים היות והטכנולוגיה כיום מגיעה לרמות מזעור מינימאליות. חשוב לציין שאין מדובר בסוף הדרך מכיוון שכבר בימים אלו קיימים מחקרים לפיתוח שערים לוגיים על אטום בודד. אולי בכל זאת יש תקווה...

כיום מערכות המחשוב ניתנות לחלוקה לחומרה ולתוכנה- החומרה נחשבת לחזקה מאוד יחסית לדרישות התוכנה, דהיינו ניתן לקנות מחשב ביתי פשוט המכיל משאבים שהם הרבה מעבר לדרישות המינימום, או הדרישות האופטימאליות של מערכות ההפעלה הקיימות בשוק. אם כך, פותח רעיון בו ניתן יהיה לנצל את משאבי החומרה באופן יעיל וזול יותר. הרעיון הוא למעשה להקים שרת (או מחשב חזק) אשר יריץ תוכנה אשר יודעת לדמות רכיבי חומרה פיזית לתוכנה, ואז ניתן לנצל חומרה פיזית אחת באמצעות רכיבי חומרה "וירטואליים" רבים. תתארו לכם שבמקום לקנות 10 שרתים פיזיים, ניתן לקנות שרת אחד חזק שעליו ירוצו 10 מערכות הפעלה בו זמנית, במצב זה ניתן להוזיל עלויות רבות של הארגון.

מושגים בסיסיים

1. **Guest**

   מערכת הפעלה אשר כלל החומרה שלה מדומה על ידי תוכנת וירטואליזציה. ה-Guest אשר נקרא גם "מכונה וירטואלית" (Virtual Machine) מכיל מערכת הפעלה אשר מורצת על גביו, המשתמשת במשאבים המדומים שהוקצו לה. לדוגמה: ה-Guest מקבל זיכרון RAM, שטח דיסק, כרטיסי רשת, מעבדים וכל משאב קלט\פלט שמחשב כלשהו מקבל. כל מערכת הפעלה וירטואלית פועלת בפני עצמה, כלומר ניתן להריץ עליה כל דבר אשר ניתן להריץ על מערכת הפעלה אשר מבוססת על תשתית פיזית (חומרה).

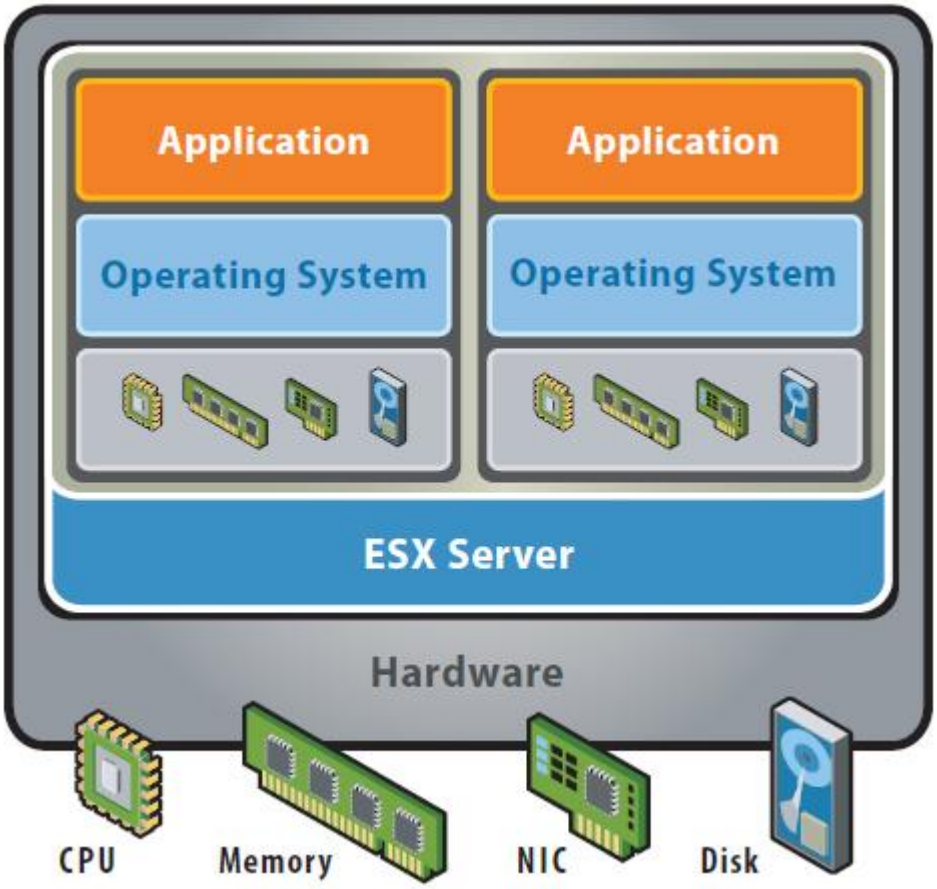
2. **Host**

   החומרה או מערכת ההפעלה אשר "מארחת" מכונות וירטואליות. ה-Host מורכב מהחומרה הפיזית של השרת ומתוכנת וירטואליזציה אשר באמצעותה מנהלים את כלל המכונות הוירטואליות.

סוגי וירטואליזציה בסיסיים

1. Type1

הוירטואליזציה הראשונה שפותחה על ידי חברת IBM, וכיום הנחשבת לנפוצה ביותר בקרב השרתים משויכת לקטגוריה הנקראת Type1. להלן מבנה כללי של קטגוריה זו:



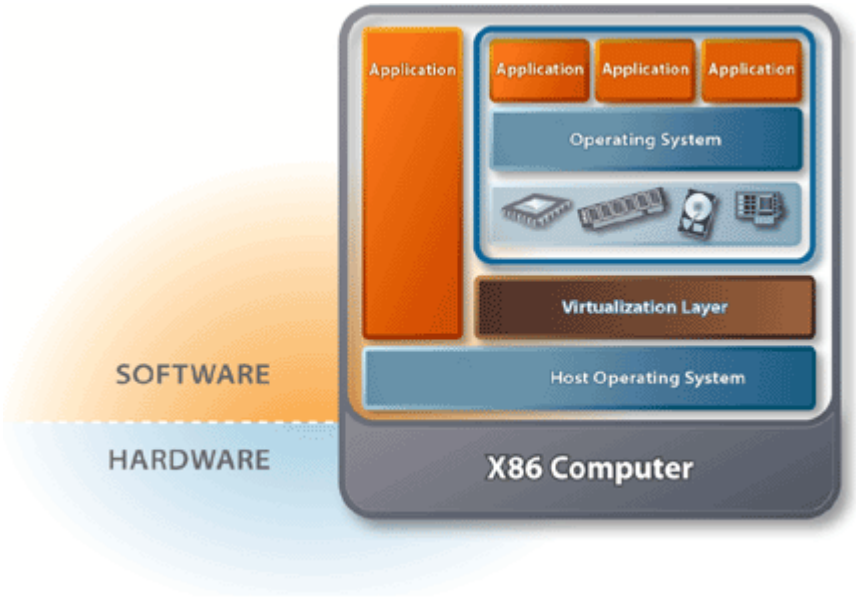
[השרטוט נלקח מאתר VMWARE]

הסבר:

וירטואליזציה זו מבוססת על שכבה מתווכת בין החומרה הפיזית של השרת (Host Hardware) למכונות הוירטואליות (Guests). השכבה המפרידה נקראת באופן כללי Hypervisor או VMM (Virtual Machine Monitor), ובמקרה הפרטי בשרטוט מדובר ב-ESX של חברת VMWARE. חשוב לציין כי קיימים "שחקנים" מובילים נוספים בשוק, כגון Microsoft Hyper-V R2 ו- Citrix XenServer.

2. Type2

כאמור, בסוף שנות ה-90 חלה עליה בפיתוח נושא הוירטואליזציה. סדרה זו של וירטואליזציה פותחה לשוק ה-Desktops שמטרתה הייתה יכולת הרצת מספר מערכות הפעלה במקביל על המחשבים הללו. להלן מבנה כללי של וירטואליזציה זו:



[קישור לשרטוט]

הסבר:

וירטואליזציה זו מבוססת על מהערכת הפעלה קיימת על תשתית החומרה הפיזית(32 או 64 ביט), כלומר מותקנת מערכת הפעלה בסיסית (Windows\Linux\Mac), ועל גביה מותקנת תוכנת וירטואליזציה. תוכנה זו דומה לעקרון ה-Type1, אולם שכבת ה-Host תופסת יותר משאבים ואף פגיעה יותר אבטחתית עקב קיום "משטח תקיפה" (Attack surface) גדול יותר. לדוגמה, ב-Type1 שכבת ה-Hypervisor תופסת מספר Megabytes, ואילו מערכת הפעלה בסיסית (כמו Windows) שוקלת הרבה יותר משמעותית. הנגזרת מכך היא יותר פונקציונאליות, יותר שירותים פתוחים ואפילו סביבת משתמש נגישה יותר למשתמשי הקצה (אם מדובר בסביבה שמותקנת על גבי תחנת קצה). דוגמה למוצרים שעובדים בתצורה זו: Microsoft Virtual PC, VMWARE Workstation\Server ו-Sun VirtualBox.

יתרונות הוירטואליזציה

1. עלויות (כפי שכתבתי)-ניתן להתייחס להוזלת ההוצאות בהיבטים רבים כגון מקום ב-Hosing, חשמל ופחות אנשי תמיכה.
2. ברוב תוכנות הוירטואליזציה קיימת אפשרות לבצע Snapshot. כלומר קיימת אפשרות לשמור "תמונת מצב" של מערכת ההפעלה - תחליף טוב לגיבוי, אך לא בכל מצב.
3. שימושי בסביבת בדיקות, לדוגמה: פיתוח אפליקציה גרם לקריסת המערכת, וניתן לחזור לגרסה הקודמת של הפיתוח או למצב של יום לפני קריסת השרת בהנחה שבוצע Snapshot על השרת.

פתרונות וירטואליזציה מכווני אבטחת מידע

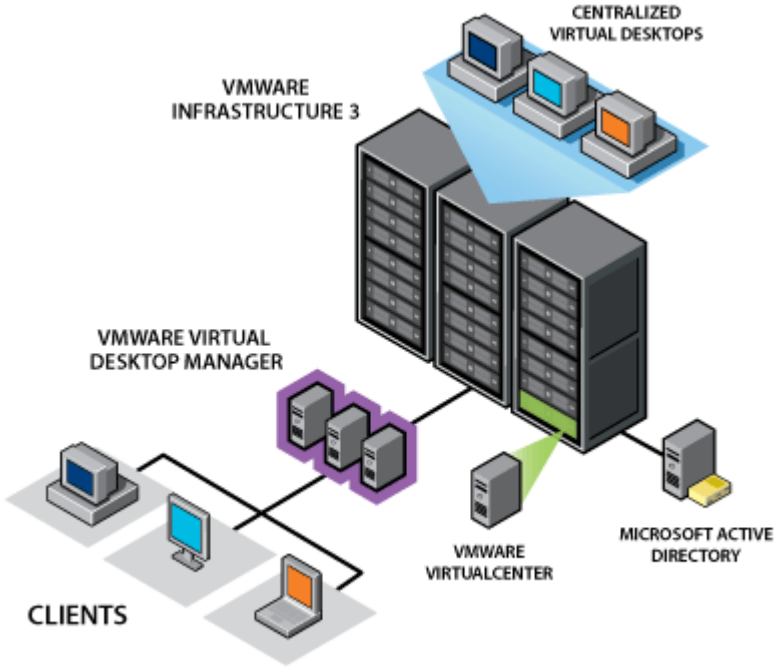
מעבר להצגת הרעיונות הקיימים ב-Type1 ו-Type2, קיימים פתרונות אשר מבוססים על וירטואליזציה אשר מטרתם (בין היתר) היא מתן מענה תשתיתי/אפליקטיבי מאובטח בארגון. אך לפני שאציג פתרונות אבטחה חשוב להציג את עיקרי הבעיות הנפוצות:

1. הארגונים כיום מתמודדים עם בעיות ניהול מרכזי לתחנות העבודה עקב אי היכולת לדעת בדיוק אילו מחשבים קיימים בתוך הרשת הארגונית ואי יכולת השליטה על כל תחנות העבודה (כדוגמת תחנות לא מנוהלות אשר נמצאות ב-Workgroup).
2. קיים קושי בהגבלת התקנים (כדוגמת USB) בתחנות העבודה, וכנגזרת מכך גם קיימת בעיה במיפוי\ניטור זליגת מידע בארגון.
3. קיימות פגיעויות רבות המשפיעות ישירות על תחנות העבודה של המשתמשים לדוגמה, ניתן ליישם התקפה על תוכנת הדפדפן של המשתמש אשר נפגעת על ידי אתר שמבצע מתקפת DNS Rebinding, שעלולה לאפשר מתן גישה מלאה למשאבים הפנימיים של הארגון מכתובות IP חיצוניות. (מאמר הנושא DNS Rebinding אפשר לקרוא בגליון הנוכחי)

להלן פתרונות האבטחה:

1. VDI (Virtual Desktop Infrastructure)

פתרון VDI הוא פתרון וירטואליזציה מסוג Client Virtualization (ידוע גם בשם Desktop Virtualization) אשר מספק למשתמשים סביבות עבודה מלאות, החל ממערכות הפעלה ועד להגדרות ואפליקציות המותאמות אישית עבור כל משתמש ברשת(יוסבר בחלק הבא של המאמר). על מנת להמחיש את הרעיון מצורפת תמונה מאתר VMWARE:



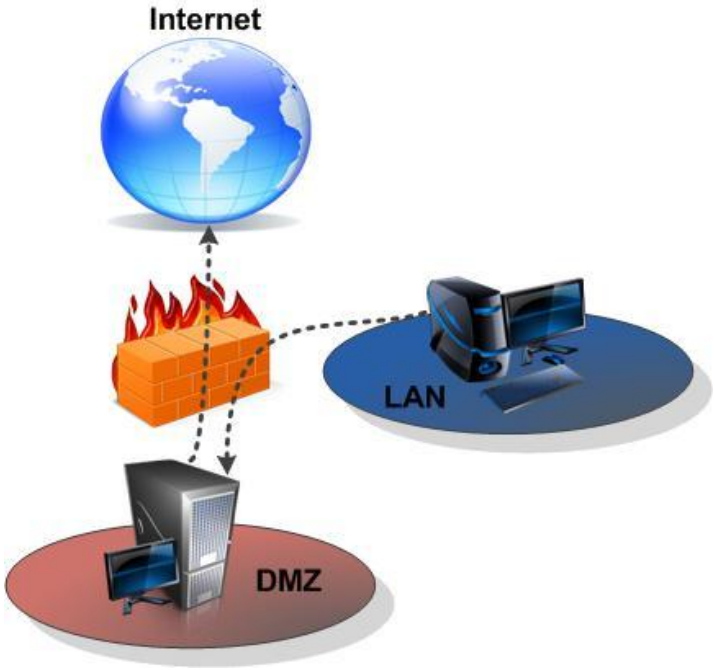
הסבר השרטוט:
בארגון קיים Datacenter המכיל תשתית וירטואלית מסוג Hypervisor ל-VDI. תצורת העבודה של תשתית VDI היא Client-Server, כלומר למשתמשים יש Client פיזי כלשהו (כדוגמת PC או Thin Client) אשר באמצעותו הם מקבלים שולחן עבודה מלא שרץ בפועל בשרת ב-Datacenter.

ניתן לסכם את יתרונות הפתרון בכך שקיימת שרידות של סביבות העבודה של המשתמשים, ניתן לנהל את סביבות המשתמשים באופן מרכזי ובנוסף ניתן להתמודד עם זליגת מידע הן בהיבט הלוגי בתשתית ה-VDI והן בהיבט הפיזי ב-Thin Clients.

2. Application Virtualization

הקדמה:

אחד הפתרונות הנפוצים להרצת אפליקציות בצד השרת הוא פתרון ה-Terminal Server (שרת מסוף). מה הוא Terminal Server? תצורת מסוף היא שיטת עבודה ותיקה בה כל משתמש מתחבר לשרת, וממנו מתבצעות כל פעולות האפליקציות שמותקנות בשרת. שיטה זו ידועה בהיבטים התפעוליים שלה המאפשרים ריכוז של תעבורה או עבודה מול אפליקציה דרך שרת יחיד (או חוות שרתים) המנוהלת באופן מרכזי. בימים אלו ניתן להתייחס לשירותי המסוף בעיקר מהיבט אבטחתי. לדוגמה, בארגון יש רשת פנימית שאינה מחוברת לאינטרנט מטעמי אבטחת מידע, אך עובדי הארגון חייבים לעבוד מול האינטרנט. במצב זה אפשרי לתת להם גישה לשירותי מסוף שיפעילו דפדפן אינטרנט כלשהו, ומהדפדפן יגלשו לאינטרנט. הערה: השרטוט הבא מהווה דוגמא בלבד, ובדרך כלל בארגונים התשתית היא מורכבת יותר מהרעיון שמוצג בשרטוט.



שירותי המסוף מופעלים במספר דרכים:

- גישה ישירות לשרת Terminal וקבלת ממשק גרפי למערכת ההפעלה של שרת המסוף, בדיוק כמו לעבוד עם Windows נוסף.
- הפצת Dashboard שלמעשה מכיל ממשק של "לוח" עם כל האפליקציות שהמשתמש מורשה אליהן.
- הגדרת תוכנות עבור המשתמשים כך שיוכלו להפעילן באמצעות ממשק Web.

הסבר הטכנולוגיה:

נושא הוירטואליזציה באפליקציות עובד באופן דומה ל- Terminal. ביישום כזה מתבצע "פרסום" (Publish) של אפליקציות לקבוצות מוגדרות של משתמשים בארגון. בטכנולוגיה זו, האפליקציה נפתחת לכל יישום אשר מותקן על גבי מערכת ההפעלה , אולם בפועל האפליקציה רצה על גבי השרת, כך שאם משאב כלשהו יפגע אז הוא יהיה שרת האפליקציה.

באותה הנשימה חשוב לציין שלא כל סוגי האפליקציות יכולות להיות וירטואלית , כדוגמת רכיב אנטי וירוס ואפליקציות שיש להן תלות כלשהי בחומרת המחשב הפיזי.

אבטחת מידע בתשתית הוירטואלית-מה עושים?

טכנולוגיות הוירטואליזציה מאפשרות שימוש יעיל בתשתיות החומרה והתוכנה, אולם הן טומנות בחובן לא מעט סכנות בתחום אבטחת המידע. בבואנו למימוש מערך וירטואליזציה נדרשת השקעת מחשבה לא רק בהיבטים טכנולוגים תפעוליים אלא גם בהיבטי האבטחה שעתידיים להתקיים במערכת, היות וככל שעולה הפונקציונאליות התפעולית תיתכנה פרצות חדשות.

דוגמאות טובות לכך, המוכרות מעולם אבטחת המידע לביצוע , הינן תכנון נכון של ארכיטקטורה , סגירת שירותים, הגבלת משתמשים, הגדרת הזדהות איכותית, ועוד.

מעבר להיבט מערכות ההפעלה חשוב להתייחס גם לנושא הוירטואליזציה של אפליקציות. בארגונים רבים משתמשים בשיטה זו על מנת לגשת מהרשת הפנימית של הארגון לאינטרנט באמצעות תוכנת דפדפן או תוכנת דואר אלקטרוני . האפליקציות רצות בפועל על שרתי האירגון , ודי ב"טעות" אחת באפליקציה או בהגדרותיה על מנת להשתלט על השרת , לדוגמה: אם הדפדפן יופעל עם הרשאות גבוהות , הרי שניתן יהיה לנסות ולנצל זאת לטובת התוקף. התוקף יכול להוריד ActiveX (או להשתמש בשיטות נוספות כגון JavaScript) באמצעות הדפדפן ובכך לקבל הרשאות ניהוליות על השרת

רצוי לאבטח את תשתית הוי רטואליזציה, באמצעות שילוב של תכנון מאובטח , טרם פריסת הטכנולוגיה, הקשחת הפלטפורמה וחיזוק בטכנולוגיות אבטחה חיצוניות . היתרון העיקרי הנובע מתכנון נכון ומאובטח הוא מימוש תהליכי עבודה מסודרים וגיבוש ארכיטקטורה , המתבססת על עקרונות Best Practices של אבטחת מידע, הקשחת מערכות ההפעלה, תשתיות תקשורת שיתופיות וכל היוצא בזאת. באם תשתיות הוירטואליזציה כבר פרוסות בארגון, אזי התהליך יהיה מעט מורכב יותר היות ותיתכנה מערכות הפעלה וירטואליות רבות שנדרש להקשיחן באופן פרטני.

היבטי אבטחה מרכזיים אליהם חשוב מאוד להתייחס בהקשחת תשתיות וירטואליות הינם: ביטול יכולת העתקת קבצים בין מערכת הפעלה לחברתה ברמת התשתית הוירטואלית, הגבלת צריכת משאבים עבור כל מערכת הפעלה ע ל מנת למנוע מתקפות כגון Denial of Service, הגדרות חיוויים (Audit) על מנת לקבל מידע על הגישה לתשתית הוירטואלית, סגמנטציה, אבטחתו של הממשק הניהולי באמצעות רשת תקשורת ייעודית לניהול, הקשחתם של תשתיות התקשורת השיתופית, שימוש בסוכני הגנה על הסביבות הוירטואלית וכמובן מימוש מנגנון הזדהות חזק כולל מדיניות סיסמאות. מעבר לכך קיימים היבטים נוספים המותאמים ספציפית עבור כל יצרן וכל גירסה.

סיכום

במאמר זה סקרנו את נושא הוירטואליזציה וראינו שהטכנולוגיה משרתת אותנו כבר החל משנות ה-60 ב-Mainframes, והחל מסוף שנות ה-90 בשרתים וברכיבי קצה. על פי המאמר ניתן לראות כי אכן מדובר בטכנולוגיה בעלת יתרונות רבים , החל מ העלויות והיבטים תפעוליים ועד למוצ רים המכוונים לאבטחת מידע. וירטואליזציה אמנם יודעת לספק פתרונות אבטחת מידע , אך נדרש הצורך באבטחת התשתית הוירטואליות עקב קיום "פונקציונאליות" אשר עלולה לפגוע ברמת אבטחת המידע.

על המחבר

ניר ולטמן, יועץ טכנולוגי בכיר בחברת Security Art בעל רקע באבטחת תשתיות ועוסק כיום במתן ייעוץ באבטחת אפליקציות מול לקוחות חו"ל.