stki.info
IT Knowledge Integrators
Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

סיכום מפגש שולחן-עגול

ניהול ותפעול תחנות קצה

מנחה

פיני כהן

Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

stki.info
IT Knowledge Integrators
Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

לקוחות נכבדים שלום,

תודה על השתתפותכם במפגש שולחן עגול Round Table בנושא ניהול ותפעול תחנות קצה.

מצ"ב סיכום עקרי הדברים שעלו במהלך המפגש. במפגש עלו נושאים מהותיים שתומצתו בסיכום כפי שעלו. אין בסיכום זה המלצה גורפת ללקוחות אלא מתן פרספרטיבה והצגה של ההתלבטויות שעלו במפגש כלומר "מהשטח".

בברכה,

פיני כהן

תוכן

Contents

בנייה והפצה של IMAGE

להלן תיאור התנהלות של הפצת IMAGES בסניפים ובמטה של אחד הארגונים – בתור פרספקטיבה. תוכנת ההפצה שבשימוש בארגון זה הנה BigFix. הארגון בונה 4 IMAGES שמתבססים על 2 MASTERS. ה- Images נבנים על ידי MDT (Microsoft deployment toolkit) של מיקרוסופט ומופצים ידנית על ידי הטכנאים (disk on key). הסיבה להפצה הידנית היא שלסניפים (בעיקר הקטנים) אין תקשורת מספיק מהירה להפצה דרך WAN.
הפצה גדולה של images -לדוגמה שדרוג מערכת הפעלה – עורכת כחצי שנה (כאמור הפצה ידנית) וזאת מכיוון שחלונות הזמן שמאפשרים עבודה אינם ארוכים.

ארגון אחר תיאר מצב שבו יש 3 IMAGES . אחד לניידים ושני סוגי תחנות עבודה. IMAGE אחד הוא רזה. IMAGE שני מכיל את רוב רובם של היישומים (בעיקר את כל היישומים שלא מחייבים התקנה ספציפית עם serial number או יישומים שעלותם גבוהה ויש לנהלם באופן ספציפי).
ה- IMAGE מתעדכן פעם ברבעון. בארגון זה מבצעים הפצה מהמרכז שמכיל את ה- image בכל סניף כאשר התחנות בסניף יבצעו התקנה ב- LAN. משך זמן ההתקנה בסניף (לאחר שה- image הגיע לסניף) הוא כשעה (שימוש ב- multicast).
ארגון אחר שהנו גלובלי תיאר מצב שבו הפצת ה- images והעדכונים מתבצעת באמצעות SCCM. ה- IMAGE הראשוני נבנה באמצעות MDT ומותקן על Win (preinstalled edition) PE שמותקן תמיד אבל לאחר מכן יש התקנה מלאה שתלויה באזור הגיאוגרפי ובתפקיד המשתמש – זאת בשילוב עם group policy שמוגדר ב- Active directory.

ההתקנה של ה- image החדש מתבצעת או על ידי התקנה פיזית מ- disk on key או על ידי PXE BOOT מהרשת שמעלה את Windows PE (pre-installed) ולאחריו מתבצעת הבחירה ב- image שיש להתקין.
לקוחות מתקינים את התוכנות הספציפיות של בעלי התפקידים השונים מעבר ל- image הכללי או באמצעות group policy ב- active directory או באמצעות הגדרה של מספר גדול יותר של images (המבססים על image משותף) אך לכל image ספציפי יהיה task sequence

ב- SCCM אשר יתקין את האפליקציות הדרושות לכל בעל תפקיד – כל זאת כחלק מהתקנת ה- image.

האפשרות לבצע את התקנת התוכנות הספציפיות באמצעות group policy הנה ותיקה ומאפשרת גמישות אולם היא מחייבת ביצוע login על ידי המשתמש הספציפי (ורק אז מותקנות התוכנות הספציפיות) ולכן עלולה לקחת זמן רב (לאחר שהמשתמש בצע Login- כי הרי לא רוצים לתת את הסיסמה של העובד לטכנאי ה- PC).

עדכוני PATCHES ותדירותם

להלן תיאור מצב בנושא של עדכוני PATCHES של אחד הארגונים. הארגון מבצע עדכוני PATCHES בתחנות הקצה פעמיים בשנה. העדכונים מתבצעים בעקרון באמצעות bigfix אולם ישנם מספר תוכנות שגם מופצות ידנית מכיוון ש- bigfix עושה עבודה פחות טובה (לדוגמה עדכוני JAVA). הארגון יבצע התקנות לעדכוני מיקרוסופט שמוגדרים כ- critical וכ- important. לעיתים מבצעים roll back לעדכונים – ברוב המקרים בהצלחה.

ארגון אחר תיאר מצב שבו ביצע עדכונים פעם בחודש אולם בעקבות מקרה ransom (אמנם ברשת חיצונית) הוחלט על ידי גורמי אבטחת מידע ורגולציה בארגון להפיץ עדכונים פעם בשבוע (דבר שמבטל למעשה את האפשרות לבצע בדיקות). ההחלטה התקבלה לא מזמן ובינתיים עומדים בה ללא בעיות מהותיות (סביר להניח שהפצה מהירה כזו תגרום לתקלה בסופו של דבר).

STKI – הנושא של תדירות עדכונים הנו נושא "נפיץ" – מצד אחד גורמי אבטחת המידע לוחצים לבצע עדכונים כמה שיותר מהר. מצד שני עדכונים אלו דורשים מאמץ וזמן בעיקר בבחינת המשמעויות של העדכונים. בכל מקרה המגמה היא של קיצור טווחים.

בדיקות לפני הפצה של patches

ישנה שונות בין הארגונים לגבי ביצוע הבדיקות לפני הפצת patches. ברוב הארגונים ישנן בדיקות מקיפות וזאת מכיוון שישנם מקרים לא מועטים שבהם עדכונים גורמים לתקלות במערכות (דוגמה מני רבות – לקוח עדכן patch של RDP וחלק מהמדפסות הפסיקו לעבוד...). הבדיקות מתבצעות במעבדה שמחזיקה כמה גרסאות של חומרה וגם 2 גרסאות

אחורה של IMAGES. שם מבצעים ניסויים של המערכות המרכזיות. לאחר מפיצים לאגף מערכות המידע, לאחר מכן 2 סניפים גדולים ו- 2 סניפים קטנים ואז (במידה ולא היות תקלות). ארגון אחר תיאר סנריו אחר של בדיקות –בונים קבוצת ניסוי של כ-10% מהמשתמשים באופן שייצג את כל הארגון. מפיצים להם את העדכונים ולאחר שבוע מבצעים בדיקה אם היו תקלות – גם מקבלים דיווח מה- service desk אבל גם מ בצעים בדיקה ב- event log של קבוצת הניסוי. ולאחר שבוע נוסף – מתקינים בכל הארגון.

הדרכות למשתמשים בהקשר אבטחת מידע

אחד הארגונים תיאר מצב שבו כל עובד בחברה מקבל הדרכות ולומדות בתחומים של רגולציה ואבטחת מידע. גם לכל עובד חדש ולאחר מכן פעם בחצי שנה. כאשר משתמש שלא מבצע הדרכה (לומדה), לאחר מספר התראות – ננעל!!

ארגון נוסף תיאר מצב שבו באופן יזום שולחים mail מתחזה ואוספים אנליזות מי המשתמשים ש"נפלו בפח".

Windows 10

רובם המכריע של הארגונים נמצאים בתהליך בדיקה והטמעה של Windows 10. התגובות הראשונות הנן ש- Win10 בהחלט בשל לשימוש. אחת המשימות המרכזיות שיש לבצע הוא העברת מערכות ה- web לתמיכה ב- IE11 מגרסאות ישנות, פעולה שלקוחות התחילו לבצע זאת כבר במהלך השימוש ב- Win7 תוך כדי הפניה מתאימה של חלק מה- URL ל- enterprise mode.

לגבי גרסת windows 10 המותקנת לקוחות מתלבטים האם להסתמך על גרסאות שמיועדות לטווח ארוך Long-Term Servicing Branch (LTSB) או להתקדם קדימה בפונקציונליות לגרסאות Current Branch for Business (CBB) – שאומנם יספקו פונקציונליות מתקדמת אבל חייבו את הארגונים לבצע שדרוגי מערכת הפעלה בתדירות גבוהה יותר.

אחת הפונקציות שנחשבות מועילות ב- Windows 10 הנה Device Guard שמשפרת משמעותית את מצב האבטחה בתחנה (הגנה משופרת על ה- kernel) אולם היא מחייבת

מעבר לסטנדרט חדש של firmware – ה- UEFI (Unified Extensible Firmware Interface) ולעיתים גם שדרוג BIOS בפועל (תלוי במחשב הספציפי שמותקן).

Power management

שימוש בפתרונות power management רווח בארגונים במטרה לחסוך חשמל. מטרה נוספת היא לשפר את רמת האבטחה כי מחשב כבוי לא מפעיל (ומפיץ) וירוסים.
לקוחות תארו מצב שבו משתמשים ב- PowerPlug הישראלי לביצוע sleep לתחנות. הפתרון מספק דוחות טובים, אפשרות לבצע חריגות למדיניות כללית (ספציפית למשתמשים שלדוגמא רוצים להתחבר מהבית בכל שעה). הפתרון מטפל בצורה טובה בהדלקת תחנות באופן ייזום שמחייבת השארת מחשב דלוק בכל סגמנט של רשת.
לקוח אחר תיאר שימוש במודול powerplan של BigFix של IBM. גם פתרון זה מתמודד עם הבעיה של הדלקת תחנות בסגמנטים שונים ברשת על ידי הגדרת "last man standing" שיודע להתמודד עם מצבים שבהם יש ניתן חשמל במחשב שמוגדר כ"last man standing". הנושא של הדלקת תחנות בסגמנטים שונים הנו אחד הנושאים המאתגרים בתחום זה כאשר אם מגיעים להדלקה של כ- 90% מהמחשבים הדבר נחשב טוב ("פעם בחודש יש סגמנט שלא התעורר").

בדיון הוזכר מוצר נוסף בשם deep freeze שמחזיר מערכת הפעלה למצב נדרש – מתאים למקומות כמו עמדות משותפות או קיוסקים שלעיתים פוגעים באפליקציות שמותקנות.

LibreOffice

לקוח גדול תיאר מצב דיי ייחודי בישראל שבו לפני מספר שנים הוחלפה בסניפים תשתית Office ל-LIBREOFFICE. מדובר על סדר גודל של מספר אלפי תחנות. לאחר מספר גלגולים שבהם היו בעיות בעברית נמצאה גרסה סבירה אשר נמצאת בשימוש עד היום אצל רובם המכריע של המשתמשים בסניף. השימוש ב- outlook מתבצע באמצעות outlook web access. הפרויקט כלל גם הסבת כל הטפסים בארגון ל- PDF בכדי לשמור על תאימות מלאה. לעיתים יש שימוש גם ב- Office Viewer בסניפים.

Thin clients

בדיון עלה הנושא של thin clients. כאשר לקוחות מתלבטים בין thin clients סטנדרטיים לבין zero clients אשר אינם מכילים GUI של מערכת הפעלה מלבד החלק שמתחבר לשרת (ל-connection broker).

– STKI

כאשר נגשים לפתרון בתחום זה מה כחשוב לזכור הוא את העיקרון של ה- trade off בתחום זה. יש את הפתרונות ה"רזים"\"מוקשחים" הנקראים בד"כ zero client – כאן מדובר על מערכת הפעלה מנוונת (אין לה ממשק למשתמש) הצרובה על זיכרון וכאשר היא עולה היא מפעילה את ה- rdp\ica client שמתחבר ישר לסביבת השרתים. בדרך כלל מדובר על נגזרות של לינוקס.

יש את הפתרונות ה"עשירים"\"כבדים" יותר המבוססים על Windows Embedded Client (מה שהחליף את xp embedded), או על לינוקס (אבל עם ממשק משתמש להתקן עצמו).

ככל שהפתרון יותר "רזה" ו"מוקשח" כך עולה רמת האבטחה ורמת הפשטות בתפעול, אבל מצד שני ישנה קשיחות בפתרון כאשר רוצים להפעיל אפליקציות ייחודיות המשתמשות ב-drivers יעודיים. דוגמה רווחת, ישנם לקוחות אשר רוצים להשתמש בכרטיס חכם לצרכי אבטחה. כרטיס זה מתממשק עם USB אבל דורש driver ייעודי ולכן לא תמיד רץ על ההתקנים ה"רזים".

ישנם התקנים "רזים" אשר לא מאפשרים תיקון כי הכל צרוב ולא מאפשר כתיבה מחדש מערכת ההפעלה (לייתר דיוק ה- kernel שרץ) ויש התקנים שכן מאפשרים "צריבה" מחדש.

מעבר לסוגיה של "כתיבת התיקון" לתוך מערכת ההפעלה (פעולה שמחייבת עבודה מול היצרן) העובדה שניתן לצרוב את המכשיר מחדש הופכת אותו במובן זה לפחות מאובטח.

לעומת זאת, במכשירים היותר "כבדים" אין בעיה להתקין את ה- driver (כמו שמתקנים ב-PC) אבל רמת האבטחה כאן פחותה לעומת המכשירים הרזים. ולעיתים צריך להתקין על המכשירים ה"כבדים" גם antivirus עם כל המשמעויות.

השחקנים הבולטים בישראל בתחום זה הנם (לא לפי סדר) הנם: HP ,BIG-LK , DELL WYSE, CHIPPC.

על שימוש ב- VDI

STKI קיימה שולחן עגול בנושא VDI שדן בעיקר בהקמת הסביבה. שולחן עגול זה נמצא ב- https://www.scribd.com/doc/38828871/Vdi-Case-Final .

כעת התקבלו פידבקים לגבי השימוש בפתרון. הפידבקים הנם חיוביים בהקשר של השימוש (בהקשר זמינות, קלות שדרוגים, חויית משתמש, DR ואבטחת מידע). אולם מדובר בהשקעה לא קטנה – יש להשתמש בחומרה (שרתים, SSD) ברמה הגבוהה ביותר בכדי לקבל ביצועים טובים.

גם בסביבת VDI ישנה סוגיה של הפצה והגדרת IMAGES. לקוח תיאר מצב שבו כיום הוא משתמש ב- SCCM לביצוע ההפצה בתוך סביבת ה- VDI ושוקל להוסיף את app volume של VMWARE . הפתרון מתקין על IMAGE נקי אפליקציות בזמן ה-LOGIN מאוד מהר. בניגוד ל thinapp שמריץ אפליקציה וירטואלית על מערכת ההפעלה פתרון ה app volume מחבר דיסקים וירטואליים שמכילים את האפליקציות אל הדסקטופ הוירטואלי בזמן LOGIN והיתרון שהאפליקציות רצות native ולכן אין בעיות של תאימות אפליקציות. התוצאה שהוא מספק ניתוק מלא בין הדסקטופ לאפליקציות שרצות עליו[1].

עם זאת יש לציין ש- VDI לא מתאים לכל האוכלוסיות לדוגמה לאנשי פיתוח שדורשים תחנה חזקה עם זיכרון רב. לגבי הפיתוח נכון להיום VDI לא תומך ב- INTEL VT ולכן לא ניתן לפתח אפליקציות למובייל (IOS ANDROID).

יש לציין שלמרות הנוחות היחסית בביצוע שדרוגים, אם יש PATCH גדול מאוד, גם בסביבת VDI לא מבצעים אותו לכל המשתמשים ביחד בגלל סוגיית ביצועים.

[1] מידע שהתקבל מהספק

תגובות של ספקים

מיקרוסופט

מיקרוסופט מאפשרת ללקוחותיה תחת הסכם ה Software Assurance לעבוד עם כל הגרסאות הקיימות והעתידיות של Windows 10 כאשר לציוד קצה ותרחישים מיוחדים כגון חדרי ניתוח או אנשי בקרה אווירית,
הכנו גרסת Windows 10 מיוחדת הנקראת LTSB אשר מאפשרות לעבוד ללא צורך בקבלת עדכונים עד 10 שנים.
יש לציין כי גרסה זו אינה מיועדת עבור ה Productivity Worker הרגיל היות והיא אינה כוללת את כל הרכיבים הקיימים בגרסה הרגילה ואשר מתעדכנים בצורה שוטפת כגון דפדפן ה Edge החדש, Cortana ועוד

Windows 10 כוללת רכיבים נוספים שבעבר הצריכו שימוש במוצרי חומרה ותוכנה נוספים כגון היכולות לבצע "חזרה לאחור" בכל אתחול מחשב כדי להסיר את כל השינויים שבוצעו בו וע"י כך לשמור על רמת תקינות ידועה, יכולת זו הייתה קיימת בעבר רק בגרסאות ה Embedded המיוחדות של המוצר ועתה קיימת בכל גרסאות ה Enterprise של המוצר.

לאחרונה הוכרז שיתוף פעולה רחב היקף נוסף עם חברת Citrix כדי להביא את בשורת ה-VDI עם Windows 10 בצורה קלה לארגונים ע"י שימוש בתשתיות מחשוב הענן של מיקרוסופט, Azure, כדי להכיר יותר טוב את הנושא אנו ממליצים על העמוד הבא - http://www.citrixandmicrosoft.com/Solutions/DesktopVirtualization.aspx

לסיכום, Windows 10 מהווה את גרסת מערכת ההפעלה המתקדמת והמאובטחת ביותר שמיקרוסופט הוציאה עבור מחשבים אישיים, היא מכילה מערכות הגנה מתקדמות, נוחות תפעול מודרנית כדוגמת דפדפן חדש ועוזרת דיגיטלית אישית, יכולות חדשות בתחום הניהול על מנת להוריד את עלויות התפעול הכוללות ותמיכה במגוון הולך וגובר של מכשירים מודרניים כדוגמת מסכי מגע, מצלמות תלת מימד ומקלדות נתיקות ועוד.
כחלק מתפיסתה של מיקרוסופט את המוצר כ- Windows as a Service, אנו נוציא בקרוב Release עדכני של מערכת ההפעלה אשר יוסיף תכונות שנתבקשו ע"י משתמשי ה-

Windows Insider ברחבי העולם כדוגמת מערכת "דלף מידע" מובנית וכן הוספת תמיכה ב Extensions לדפדפן ה Edge החדש.

NessPro

מדידת ההשפעה העיסקית של השינויים בתחנות הקצה

כאשר אנו בונים ו/או משנים את תחנות הקצה, עלינו לקחת בחשבון את השיפור שאנו מעוניינים לתת למשתמשי הקצה ולהיות מסוגלים לתת תיקוף להשפעה העיסקית של השינוי על משתמשי הארגון.

ניהול ותפעול תחנות הקצה נועד, לאפשר למשתמשי המחשב בארגון "משתמשי הקצה" סביבת עבודה נוחה ויעילה, כדי לאפשר למשתמשים לעשות את עבודתם ביצירת הערך לארגון.

כדי לאפשר זאת, עלינו לנטר באופן קבוע את חווית השימוש, של משתמשי הקצה, במחשוב האישי ולבחון כל שינוי בעמדות הקצה, כיצד הוא משפיע.

לבדוק את ה"לפני ואחרי" השינוי, להיות מסוגלים למדוד באופן מדוייק, מה המשמעות של כל שינוי על יעילות העבודה, תוך תפיסת ROI כוללת: גם של מחיר השינוי וגם ההשפעה על המשתמש.

נספרו מציעה את מערכת אטרניטי כמערכת היחידה הקיימת כיום ומאפשרת מדידה אמיתית של חווית המשתמש.

המערכת מודדת את הפעילות שעושה כל משתמש (לכל המשתמשים בארגון) על תחנת הקצה ומאפשרת לקבל תמונה אמינה על הזמן הממוצע שלוקח, למשתמשי הקצה, לעשות כל פעילות עיסקית . כך לקבל מדד אמין וחד ערכי להשפעה של כל שינו, בתחנות הקצה, על יעילות העבודה של המשתמשים.

מערכת אטרניטי מאפשרת לבצע מדידה על כל סוג חומרה ועל כל סוג של טכנולוגיה ובנוסף לחווית השימוש לקבל תמונה מלאה על כל מה שמתרחש בתחנת המשתמש בעת ביצוע העבודה השוטפת. לדעת מה היה השימוש במשאבים, איזה Process רצו ברקע, אם היו קריסות או איטיות ממה הן נבעו ועד

המערכת תומכת בכול סוגי תחנות הקצה כולל תחנות עבודה, מחשוב נייד, VDI, Citrix וכן במשתמשי Mobile .

Aternity, אירחה לאחרונה אירוע ייחודי לקבוצה נבחרת של מנהלי IT בכירים, בנושא שיטות עבודה מומלצות לגבי תיקוף (validating) ההשפעה העסקית של חדשנות בתחום ה-IT, המתאפשר באמצעות ניטור חוויית משתמשי קצה. שני דוברים מבנק ברקליס העולמי, הסבירו לקהל כיצד Aternity אפשרה להם לממש את היתרונות הבאים:

- הצדקת היתרון שיש ליוזמות בתחום ה-IT לגבי העובדים והעסק.
  הפחתת עלויות תפעול ואספקה תוך שיפור רמות שביעות הרצון של הלקוחות.
- ניהול IT פרואקטיבי ממוקד-משתמש, באמצעות הבנה קלה של ביצועי משתמשי קצה והשגת התרעה לגבי בעיות לפני שיש השפעה על שירות ה-IT והפרודוקטיביות של העובדים.
- תיקוף יוזמות לניהול שינויים על ידי הבנת ההשפעה על חוויית משתמשי הקצה ופעילויות עסקיות קריטיות

לסיכום:

הפתרון של חברת -Aternity מאפשר "לערוב לשינוי" המתבצע ב"מגדלים טכנולוגיים" ולספק עובדות ומדדים כמותיים, לא מדדים סובייקטיביים, כיצד השינוי משפיע על אספקת השירותים לעובדים ולמשתמשי הקצה.

למידע נוסף ניתן לפנות לחברת נספרו

אבנר מימון