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

IT procurement - Security and networking

רכש אבטחת מידע ותקשורת

יולי 2014

מנחה:
סיגל רוסין
פיני כהן

לקוחות נכבדים שלום,

תודה על השתתפותכם במפגש שולחן עגול Round Table בנושא רכש אבטחת מידע ותקשורת IT Procurement - Security and networking.

מצ"ב סיכום עקרי הדברים שעלו במהלך המפגש. במפגש עלו נושאים מהותיים שתומצתו בסיכום כפי שעלו. אין בסיכום זה המלצה גורפת ללקוחות אלא מתן פרספקטיבה והצגה של ההתלבטויות שעלו במפגש, כלומר "מהשטח".
משתתפי השולחן העלו כי חשוב שיהיה קשר רציף בין אנשי הIT והטכנולוגיות לבין אנשי הרכש על מנת להגיע למשא ומתן משמעותי ואפקטיבי בזמן רכישת מוצר. בשנים האחרונות בעקבות נושא הסייבר עלה תקציב אבטחת מידע בארגון באופן משמעותי, וכן ישנם המון מוצרים נישתיים וסטרטאפים בתחום.
בנוסף, חשוב לשקול שימוש בקוד פתוח מבחינת אבטחה בתחומים נקודתיים, וכן בתשתיות הקריטיות של הארגון. בפועל השימוש בפתרונות ממשפחת הקוד הפתוח הופך להיות נפוץ יותר ויותר.
לגבי סטארטאפים המצב דומה לקוד הפתוח, אך אין לשכוח כי אותו סטרטאפ עלול להירכש ע"י יצרן גדול וההסכם עלול להשתנות בהתאם. יש לקחת זאת בחשבון לעתיד מבחינת ניהול הסיכונים ובניית הסכם הרכש.

נקודה נוספת שעלתה בדיון הנה החשיבות הגוברת של תחום הסייבר. נראה כי בשנה האחרונה נושא הסייבר והאבטחה קיבל תקציבים גבוהים מאוד ויש ודאות רבה שהנושא ימשיך לקבל תקציבים כאלה לפחות בזמן הקרוב.

בברכה,
סיגל רוסין ופיני כהן

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

תוכן עניינים

שימוש בקוד פתוח

אחד הנושאים שעלו בדיון הוא השימוש בקוד פתוח בקרב מוצרי אבטחה וסייבר. כרגע ישנם הרבה נושאים חמים בהקשר לקוד פתוח גם באבטחת מידע וגם בסייבר (בתחום אבטחת מידע ישנם יותר פתרונות מתחום הקוד הפתוח).

בדיון הושמעו מספר דעות בנושא מהותי; אחד הלקוחות מציין כי לדעתו ישנה בעיה בנושא קוד פתוח באבטחת מידע, במיוחד לאחר תקרית OPEN SSL שהייתה לפני מספר חודשים. לדבריו לנו כארגונים קשה מאד לסמוך על יצרנים העושים שימוש בקוד פתוח, במיוחד בתחום אבטחת מידע הקריטי לארגון. לדוגמא, לדעתו יש בעיה בהעברה מאובטחת של קבצים רגישים בארגון תוך שימוש במוצר קוד פתוח במיוחד אחרי התקפת HEARTBLEED. לדבריו יש אפשרות לשימוש בקוד פתוח במוצרים פחות קריטיים לארגון כמו למשל מוצרים לאיסוף לוגים- SIEM. הסכנות בקוד הפתוח הן שקשה לדעת מי פיתח את זה, אילו שימושים נעשו בקוד בדיוק ולאילו מטרות.

אחד הלקוחות העלה את סוגיית ההתמודדות מבחינת אבטחה עם השימוש בקוד פתוח בתוך מוצר. למשל, פרצת OPEN SSL הייתה ידועה במשך שנתיים וניצלו אותה, במקום להודיע ללקוחות. זו בעיה מהותית בקוד פתוח. המוצר שהארגון עושה בו שימוש להעברת קבצים החוצה הוא מאד קריטי, ואם המפתחות נמצאים במקום אחר, התקשורת כבר לא מוצפנת.

מצד שני, לקוח אחר טוען כי דווקא בקוד פתוח יש יתרון גדול, מכיוון שיודעים בדיוק איפה הקוד נמצא, והוא נמצא בבקרת איכות של הקהילה כל הזמן היות והכל מתפרסם בשקיפות בפורומים. כל עדכון עולה לאוויר ע"י בקרה בכל הקהילה. זה דווקא לדעתו יותר בטוח לעומת היצרנים הגדולים שגם שם יש תקלות ועדכון גרסאות והכל תלוי בכמה מהנדסי ארגון.
לדברי לקוחות יש חברות שמתמחות בשימוש בקוד פתוח בארץ, אך אין הרבה חברות שנותנות לכך תמיכה. במידה ויש בעיה בקוד הכל מתנהל דרך הקהילה. אם מדובר בחברה שמגבה את הקוד הפתוח התמיכה לכך יקרה יותר.

חברות האינטרנט יכולות לעשות שימוש בקוד פתוח ולתחזק אותו בפיתוח. כאשר יש שילוב של קוד פתוח עם חברה שתומכת במוצר לגיבוי, המצב שונה וכך נוח יותר להטמיע אותו.
כמו כן עלתה השאלה האם יש מדיניות מסודרת בנושא קוד פתוח?
במערכות סגורות כמו אורקל, מיקרוסופט וMF עלויות התחזוקה והתפעול עצומות. ניתן לעבור ללינוקס (קוד פתוח) וכך לא לשלם על רישוי אלא על שירות. המשמעות במקרים אלו גדולה ותלויה באילו נושאים לעבור לקוד פתוח, למשל בשכבת מערכת ההפעלה. יש הבדל עצום בין השכבות/המערכות, וניתן להקפיא תצורה וכך לא להיות תלויים בספק. היתרון הגדול הוא בהורדת עלויות בצורה משמעותית, אבל שוב עולה השאלה מתי כן להיכנס לזה ומתי לא. בסופו של דבר הכל מתנקז לניהול סיכונים של המנמ"ר. התהליכים מאד ארוכים והטריגר לזה הוא רק כסף. דוגמאות לכך ניתן לראות ברשויות בחו"ל אשר כבר מיישמות אפליקציות בקוד פתוח ולינוקס, והמגמה רק הולכת וגדלה. כעת ניתן לראות זאת גם בנושאי התקשורת- הSDN וOpen Flow.

נשאלה השאלה בדיון- האם נתקלתם במוצרי אבטחה מבוססי קוד פתוח? אחד הלקוחות ציין כי הארגון עושה שימוש במוצר הנקרא Openbus- סורק קוד פתוח לשרתים. יש לשקול שימוש במוצרי קוד פתוח מבחינה ארגונית באבטחה גם בחלקים נישתיים יותר בארגון.

STKI: כל הנאמר בדיון הנו רלוונטי לסיטואציה, אך באופן כללי ישנה בשוק מגמה של שימוש הולך וגובר בפתרונות מתחום הקוד הפתוח, וסביר להניח שמגמה זו תגיע לאזורים נוספים בתחום אבטחת המידע.

רכישת סטרטאפים בנושא האבטחה והסייבר

נושא נוסף שעלה בדיון מתייחס לפתיחות של הרכש, ובכלל הטכנולוגיות, לכיוון הסטרטאפים באבטחת מידע. חשוב לפתוח ולעדכן כמה שיותר את אנשי הטכנולוגיה בנושא הרכש, החלופות למוצר והמשא ומתן סביב המוצר. אין להיות מקובעים לטכנולוגיה אחת. יש פה בעיה מובנת של היפתחות לדברים חדשים, לעומת מערכות ה- mainstream . חשוב לראות בכל נקודת זמן איך פותחים את הארגון לכמה שיותר אופציות.

השאלה היא כמה מוכנים להשקיע בחברת סטרטאפ? גם אם המחיר נמוך יחסית, השאלה היא מה מחיר הטעות ביישום מוצר שלא מוביל בשוק, אך כן מבטיח הרבה. ניתן לצמצם מחיר טעות אם זה נעשה בתחום נישתי. מומלץ להתחיל ביישום של מוצר לפרויקט קטן ומצומצם, וכך להבין האם יש פה טכנולוגיה שכדאי להשקיע בה.

אחד הארגונים תיאר מצב שבו בארגון ישנה רכישה רבה של סטרטאפים וישנה עדיפות למוצרים בהם מנותחת התנהגות העובד והרשאות בנוסף ל-IDM שמנוטר כל הזמן. כאשר עולה צורך בארגון הוא מגיע בד"כ מאנשי הטכנולוגיה, כאשר גוף הרכש מנתח יחד איתם באילו עסקאות כדאי להשקיע ולהתמקצע. השאלה היא האם מוכנים עבור אותו צורך לקחת את הסיכון להכנסת סטרטאפ. ברור שאם מדובר על תשתית קריטית בארגון, כמו למשל פתרון לתעבורת סלולר, לא היינו פונים לסטרטאפ.

ארגון אחר תיאר מצב שבו הדילמה גדולה כי יש הרבה התנגדויות וויכוחים בין טכנולוגיות לרכש. כרגע הם בוחנים 5-6 סטרטאפים במקביל, וכמובן שלא סוגרים בסוף עם כולם. האם מימד "הסטרטאפ" משפיע על הרכש בארגון? למשל, אחד הסטרטאפים שהארגון רכש (CYVERA), נרכש מאוחר יותר ע"י Palo Alto בעשרות מיליונים. כיום הפתרון פרוס, עובד וכולם מרוצים. למעשה הארגון נתן פתח לאותו מוצר והוא מוביל בתחומו. באותו מקרה ההסכם המקורי עדיין בתוקף, ולכן הם נהנים ממחירים טובים במיוחד. במידה ואותו יצרן שרכש את הסטארטאפ יחליט לשנות את החוזה, ייפתח תהליך רכש חדש. חשוב לבדוק אם לאותה חברה שרכשה יש עסקים נוספים עם הארגון וכך זה יכול להקל על הרכש. יכול להיות מצב בו קיימת יישות משפטית נפרדת וחדשה, ולכן קשה לקבע חוזים כאשר רוכשים את הסטארטאפ. יכול להיות מצב בו לאחר מספר שנים שהארגון נהנה מתנאי העסקה המקורית, היצרן החדש מנסה להגיע להסכם חדש עם תנאים חדשים. כאן גוף הרכש נכנס לתמונה ובודק אם יש לו כלי מינוף על אותו יצרן. במידה ולא אז ניתן אפילו להפסיק את השימוש בפתרון. הדבר קרה לדוגמה עם הסטרטאפ JUNGO שנרכש ע"י סיסקו, וזה עזר לרכש בתמחור היות ולארגון יש עסקים נוספים עם סיסקו. דוגמא נוספת- הסטרטאפ ArcSight (נרכש ע"י HP)- הAppliances בהתחלה היו של DELL,

ולאחר הרכישה היה צריך להחליף את כולם לHP. HP דרשו מלקוחות להחליף הכל ולשלם מחדש על ArcSight, אבל הארגון לא ויתר היות ויש לו עסקים נוספים עם אותו יצרן. הכל יכול לקרות, כולל גם הפסקת התמיכה במוצר ואז הארגון בבעיה.

לקוח נוסף העלה בדיון כי זיהה סטרטאפ בעל פתרון למייל מאובטח בשם SAFE-T עוד בתחילת דרכו, שהיה מאד מוצלח עד לרכישתם ע"י IBM. בדיון בלט הנושא כי כל יצרן גדול הרוכש מוצר קטן או נישתי, ינסה כעבור זמן מסוים לשנות את החוזה לארגון ולקבל יותר כסף.

בכנס הסייבר הארצי האחרון היו למעלה מ-70 סטרטאפים חדשים בתחומי האבטחה, דבר המצביע על ההתפתחות המשמעותית בתחום. לקוחות ציינו כי הסטרטאפים מחפשים בעיקר רפרנסים להתקנות בארגונים ופחות השקעה כספית. הלקוח ציין דוגמה לסטרטאפ לנושא אנומליות (זיהוי הקלדה) שלא נקנה בסוף, לא בגלל שהטכנולוגיה לא טובה, אלא כי הם חיפשו מוצרים בנושא אבל לא היה חובה לרכוש אותו, וכאן נחסך השקעה וזמן של אנשי הצוות. כיום ישנם המון סטרטאפים בנושא הגנה על סלולר. הם מגיעים לארגון ונבחנים, חלקם תומכים רק בחלק ממערכות ההפעלה, והכל תלוי בכמה מכשירים יש בארגון ולאיזה כיוון הולכים. במקרים אלו חשוב שיתוף פעולה עם היחידה המקצועית אחרת ייווצרו התנגדויות כי הרכש לא רואה הכל באותה עין.
עוד עלה כי אי אפשר לקנות הכל וליצור שכבות על גבי שכבות, היות וצריך לתחזק הכל. אי אפשר להיות מכוסים מכל הכיוונים בעולם הסייבר. צריך לדעת לנהל את מהלך הרכש נכון.
גם היום בנושא הגנת הסלולר בודקים מול 2-3 מתחרים יחד עם היחידה המקצועית. ישנה תופעה של סטרטאפים שבאים מראש עם אינטגטרטורים גדולים כמו WISE, בינת וכד', שיודעים איך הארגון עובד. הסטרטאפ רואה כי קשה לו להפיץ את עצמו לבד ובמקרה זה הרכש יותר בעייתי. האינטגרטור מכיר את רשת הארגון ואיך הכל מתנהל מבחינת החוזים וכאן קשה להוציא עסקאות במחירי סטרטאפ. סטרטאפ רוצה להיות חלק מהארגון אפילו כמעט בעלות אפסית, אך אם הוא מגיע עם אינטגרטור האחוזים מתחלקים.
סטרטאפ צריך את אתר הארגון עבור מוצר הבטא שלו, POC, QA, השאלה באיזה שלב נמצא אותו סטרטאפ, האם הוא בשל, איפה הוטמע כבר וסדר גודל הארגון בו הוטמע.

לקוחות חזרו וציינו כי הרכש צריך להיות גמיש ולא לקחת רק את היצרנים הגדולים עליהם הוא סומך, אלא לנסות לבחון טכנולוגיות חדשות ולא "להרוג" את אותו סטרטאפ. המפתח פה הוא שילוב הרכש

מההתחלה וראייה יחד את כל אילוצי השוק והאילוצים הטכנולוגיים, ואז ניתן לדעת עם איזה יצרן ללכת. נקודה מרכזית היא ניהול הסיכונים ברמה הטכנולוגית ובחירה האם להמשיך עם אותו סטרטאפ. חשוב להבין כי ניהול הסיכונים הוא טכנולוגי, נעשה POC לפני ונבדוק שכל מה שהוצג במצגת אכן בוצע. נבדוק אם הספק יציב ואם אנשי הטכנולוגיות מרוצים, ולאחר מכן אפשר להתקדם.

שאלה שעלתה בדיון: באיזה מחיר היינו מוכנים לקבל סטרטאפ? השאלה פה היא לא המחיר, אלא מה היתרון הטכנולוגי של אותו מוצר. אם המחיר יותר זול לעומת מוצר של יצרן ידוע, אז בודקים את חוסן החברה. לאינטגרטורים בארץ יש את החושים הכי טובים היות והם מטמיעים מוצר שהם מאמינים בו במובן הטכנולוגי, אחרת ייתנו לך מוצר אחר.
אם לוקחים סטרטאפ ומשלבים אותו בתוך מוצר יש המון מגבלות שיכולות להפיל עסקה מבחינה משפטית. אצלם בארגון המחלקה המשפטית מאד חזקה. כל החלטה כזו יש לה השלכה לשנים קדימה והכל בשילוב איתם. זה מאד משפיע בשילוב סטרטאפ בחברה גדולה, למשל כלים חדשים שעושים בהם שימוש שיכולים להוות מכשול. חשוב ללקוח לדעת מה הוא מקבל בסוף.

משמעות הרכש בארגון

בדיון עלה כי מחלקת הטכנולוגיות מבצעת באופן עקרוני את הבחירה של המוצר אך הרכש מעורב בנושא. הטכנולוגיות נותנות מפרט למוצר והרכש בוחן בהתאם. יכול להיות שאותו פתרון של סטרטאפ נכלל כבר באחד המוצרים הארגוניים ברמה אחרת, ולכן חשוב לקחת זאת בחשבון ולא לרוץ לקנות מוצרים.הרכש חייב להכיר את השוק והחלופות בו. פה השאלה איך מסתכלים על הרכש; רק קונה מוצרים או גם מעורב בבחירה ובהחלטות מבחינת המחיר?
לרכש יש ערך מוסף לארגון בתהליכי העבודה בארגון. יש מקרים בהם הרכש וה-IT לומדים יחד מוצרים וסך הכל זה משרת את האינטרסים של כולם. אם הקיבעון מוביל בארגון יש לנסות לפתוח את הראש. ישנם מצבים בהם איש הטכנולוגיה יעדיף מוצר שהוא מכיר למרות כל החלופות, ואז יראה כי הוא יותר יקר ב30% וייקח זאת בחשבון (הרי כולם שותפים יחד לתקציב). בארגון אחר אנשי הטכנולוגיה גם בוחרים את המוצרים וגם משווים עלויות, עושים חישוב של הכל ומה שמתאים מוציאים לרכש.

בארגונים המתקדמים יותר יש עירוב של הרכש החל משלב הגדרת הצורך, ולא רק בסוף הפעולה של בחירת המוצר. זאת לעומת מקומות שבהם האיש טכני עושה את הבדיקה הראשונית ונותן חלופות

למוצר ומעביר לרכש. כמובן שהדבר עדיף פחות על פני פעולה יחד של הרכש והIT בכל השלבים של תהליך הרכש.
חשוב ללמוד את היצרנים לאן הם הולכים ואילו מוצרים יש להם (אפילו עתידיים). לא הכי חשוב כמה המוצר עולה בסוף ברמת שורת ההזמנה , אלא ה"מסביב": קורסים, התמקצעות, טכנולוגיות, חדשנות, פי'צרים נוספים.

אחד הארגונים תיאר מצב שבו התרבות הארגונית שונה ואנשי הרכש רק חותמים בסוף על ההצעה. באותו ארגון היה מכרז כללי לתקשורת ו-HP נבחרו, כאשר הגורמים הטכניים היו מאוד מרוצים. הארגון מספר כי ערך מספר מכרזים בנושא אבטחה לאינטגרטורים ותחתיהם יצרנים בינלאומיים. במכרזים הוגדרו אבני דרך ובסופם התשלום עבר רק לאחר מבחני הקבלה של המוצר. לא משנה המוצר והמורכבות שלו. אבני הדרך שהוגדרו במכרז הן בהתאם לתוצרים, למשל רישיונות בשרת, התקנת רישיונות, אינטגרציה וכדומה. לכל שלב נכתב אחוז התשלום שמקבלים עבורו בסוף. למעשה האינטגרטור יחד עם היצרן מממן את כל תהליך ההטמעה ורק בסוף מקבל תשלום. לפי הלקוחות האחרים זה לא הגיוני, היות ויש לשלם חלק יחסי אחרי כל שלב במכרז. מה שקורה פה זה שהלקוח משלם על כל תהליך ההטמעה כי הכל נעשה יחד עם האינטגרטור.

בדיון עלה השוני בין ארגונים פרטיים לבין ארגונים ציבוריים המחויבים לחוק המכרזים הממשלתי. סט החוקים במכרז ציבורי שונה מהפרטי, כאשר יש בעקרון יותר כוח בקבלת ההחלטות למחלקת הכספים, הרכש והמשפטי. אם משנים משהו במכרז זה יכול להיות משפטי ובעייתי.

כניסה לפרויקט חדש

בדיון הועלתה נקודה בה אחד המשתתפים מספר על הדרך לכניסה לפרויקט חדש. בארגון עושים מכרז לבדיקת טכנולוגיות מתקדמות, לא COMMODITY, ועשו זאת למשל בNAC וב- SIEM. בפרויקטים חדשניים ביותר העסקה בנוייה בצורה כזו שמתבצע POC ואם הוא מצליח הספק מקבל את ההזמנה ועלות הPOC מקוזזת. אך אם ה- POC לא הצליח, הארגון משלם רק על הPOC עצמו, והוא לא חייב לכלול את אותו הספק במכרז (הספק אפילו לא מקבל הזמנה). אחרת מאבדים את כל ערך הרכש, ולכן POC הוא תנאי לקבלת הזמנה ומתומחר במכרז. POC מתומחר בעזרת הגורמים הטכניים בארגון ובודקים כמה אנשים טכניים דרוש וכמה זמן . היצרן ישאיל הכל לארגון כולל רישיונות וציוד- פה אין רכש בכלל. רק במידה וה- POC הצליח המכרז מתחיל והוא מתומחר, אחרת המכרז נכשל והיצרן לוקח הכל

ומקבל תשלום רק על עבודה. השוק התכווץ ב3 שנים האחרונות ואין הרבה אינטגרטורים טובים. צריך לשמור על מי שיש. ישנם הרבה פרויקטים וקשה לתחר בין מספר אינטגרטורים מועט.

לקוחות תארו מצב שבו בפרוייקט מתגלגל ישנם פערים בין האתרים השונים מבחינת קביעת מועד תחילת האחריות. אחריות התוכנה מתחילה "לפעול" מיידית באתרים שבהם הותקנה המערכת בתחילה, אבל באתרים שהותקנו בסוף הפריסה, שנת האחריות (או 3 השנים) מתחילה "לפעול" במועד מאוחר יותר, ולכן ישנה אי אחידות בקביעת תום מועד האחריות הכללית בארגון. הפתרון הוא לשלם על החלק היחסי, ואז מיישרים קו- סוף שנה או תחילת שנה וניתן להתגמש פה. יש יצרנים בעייתיים פה כי מכירים רק שנתי אבל הכל אפשרי.

החוכמה פה היא לעשות בדיקת נאותות למוצר בכמה רמות (בעיקר ברמה הטכנולוגית) ועם האינטגטרטור. אם האינטגרטורים החזקים באים ותומכים בזה הם לא מסתכלים רק על אותה עלות קטנה מהסטרטאפ אלא ברמה אסטרטגית יותר לעתיד. בארגונים גדולים כל תהליך רכישה כזה הוא מעל 5-6 שנים. נכון שזה סיכון לפעמים אבל הסטרטאפ מגיע עם טכנולוגיה ייחודית ואפילו ליצרנים הגדולים אין פתרון כזה. למשל בפרויקט NAC הארגון בחן 2-3 מתחרים ולא רק את היצרנים הגדולים.

לקוח אחר טוען כי אם ההבדל הוא במיליוני דולרים לא נלך עם מוצר זול כי זה משמעותי יותר אם תהיה נפילה שלו בארגון. בעלות נמוכה ובאזורים ספציפיים כן נאפשר לעצמנו לקחת מוצר סטרטאפ וללכת בבטחה. תמיד ניתן לעשות בדיקה של אותו מוצר בתיחום מסוים ואפילו לרתום את אנשי הטכנולוגיות להיפתח פה.

הערך המוסף של הרכש זו שיטת התמחור ולא הכסף. למשל, NAC רצו לעשות את הפתרון ברמת רישוי קצה ורישוי אתר והאלטרנטיבה הייתה פתרון Appliances, אבל הארגון לא רצה Appliances. הארגון בחר בתמחור ברמת ארגון SITE LICENSE. הפואנטה הייתה מודל התמחור, היות וכרכש לא ניתן תמיד לדעת אם הארגון ירצה Appliances וכמה ירצו בעתיד (במיוחד רשתות שונות).

במידה והמוצר נכשל או נופל עוד שנתיים יש פה עלות מעבר למוצר חדש, וזה שייך לניהול סיכונים. לכן, לרכש יש ערך מוסף לתחקר ולהציף את הנושא מההתחלה בניהול סיכונים ושיטת תמחור.

אחד הלקוחות נמצא כרגע בחיפוש אחר פתרון להקשחת שרתים, היות ו-NETIQ Novell כבר לא נתמכים היום. יש פתרונות נוספים של CA, סימנטק וכדומה. ישנה חשיבות להטמעת פתרון רוחבי ויישום של אנשי צוות. כמו כן, הארגון נתקל בבעיה מבחינת תעודות SSL. ביצעו הנפקת תעודות של Verisign, אשר נרכשו ע"י סימנטק, והמחיר עלה פי 3 לתעודה ל-3 שנים. כמות התעודות בארגון גדולה ולכן חשוב לבדוק יצרנים נוספים.

רכש תקשורת

בדיון עלה נושא הרשת המעורבת והגיוון ביצרנים שונים. אחד הלקוחות סיפר כי שנים הם היו מבוססים רק על ציוד סיסקו, והיוזמה באה מהרכש עם הרבה התנגדויות טכנולוגיות לשינוי, אבל הרכש מעורב והוא גם טכנולוגי. הרכש סגר את ההסכם עם סיסקו (המשיך בחלק מהרשת) ובמקביל עשו עם HP הסכם עם אותם אינטגרטורים. כאשר הארגון היה בהסכם עם 2 ונדורים היה לו יותר קל להשוות בין פתרונות בעזרת אותו אינטגרטור. נראה כי "המספרים מדברים בעד עצמם". התגלו הפרשים עצומים אשר לא הצדיקו להמשיך רק עם סיסקו. לכן, הארגון קיבל החלטה לפתרון ביניים בו במרכז שמו סיסקו ובקצוות מתגי HP. בסופו של דבר שני הונדורים לא היו מרוצים. אין בלעדיות לאף אחד וכך הרכש היה מרוצה. הקושי הגדול היה בתוך הארגון לשכנע את האנשים טכניים לנושא ולהביא לידיעתם את ההפרשים הכספיים. חשוב שיהיו אנשים טכניים שיבינו את מזעור הסיכונים ויהיו בעלי פתיחות טכנולוגית. נראה כי הסכם מסחרי עסקי קדם לטכנולוגיה במקרה זה וגם לעתיד.

כיום יש 3 רשתות: HP טהורה היות והיא יותר זולה ואין חשיבות לBACKBONE, טלפוניה IP (לא שמו סיסקו למרות הלחץ מהיצרן), אלקטל ואינטגרטור אחד לכולם. כרכש הייתה חשיבות לאינטגרציה בכל היצרנים. ישנה רשת נוספת מבוססת סיסקו. היום הרשת יציבה וכבר 4 שנים הכל תקין, והעלות ירדה משמעותית. תמיד ניתן לכופף יצרן ע"י שימוש ביצרן מתחרה לו. הכל שאלה האם שווה ליצרן להמשיך להתמודד פה מול גודל הארגון.

מצד שני, לקוח נוסף סיפר כי גם הם היו מבוססים רק סיסקו והעבירו הכל ל-HP כולל backbone. אותו ארגון לא אוהב לערבב יצרנים, כאשר כל שלב מוציאים סיסקו קיים בסניפים ומחליפים ל-HP. ישנם מתגים ישנים מאד של סיסקו שעדיין עובדים, אבל כיום אין תחזוקה לציודים ישנים, מקסימום מחליפים למתגי HP חדשים.

האם משלמים תחזוקה לציוד תקשורת כשנגמרת האחריות? לא. כיום אין תחזוקה לציוד סיסקו. יש עדכוני תוכנה ו- FIRMWARE, אבל רק ל-ROUTER וFW. לדעתו אין צורך בעדכון תוכנה אפילו. לקוחות אחרים טוענים כי הם משלמים על תחזוקה לפחות ל-3 שנים יותר, אבל על מתגים מרכזיים בלבד.