

הגנה על חדר המחשב

התקפות ממוקדות, בו זמנית, על מספר מרכזי מחשוב אסטרטגיים יכולות לשתק את הכלכלה הלאומית ואולי, העולמית. עובדה היא שממשלות בעולם המערבי מקימות גופים ורשויות ממשלתיות כדי להילחם במתקפות אלו.

התקפות סייבר הן א-סימטריות. כלומר, הן יכולות להתבצע על ידי אנשים פרטיים, קבוצות קטנות או מדינות בהשקעה קטנה יחסית. אך להתגונן מפניהם הוא עניין יקר מאוד.

במהלך השנים האחרונות, שינה האיום את פניו. אם בעבר הפצחנים (האקרים) היו צעירים עם כוונות להפגין את כישורי התכנות שלהם, היום הפצחנים נמנים על קבוצות מאורגנות עם מניעים פוליטיים, לאומיים או כלכליים.



יגאל שניידר

המתקפות האחרונות על חברות בארה"ב על ידי פצחנים המזוהים עם ממשלת סין (לכאורה) כפי שדווחו בעיתונים ממחישה שטרור הוא משהו שמנהלי IT חייבים לקחת בחשבון. פשעי סייבר גם הם נפוצים היום. בניגוד להאקר של שנות ה-90 שרצה רק פרסום, פושעי הסייבר של היום לא מעוניינים להיות בעין הציבור.

החזית הוותיקה ביותר בהגנה על חוות השרתים היא החזית הפיזית - כלומר מניעה של ניסיונות לחידרה או פגיעה בחוות השרתים מתוך כוונה לגנוב מידע או להשבתה. היום ניתן לבצע זאת מבלי להשיג גישה לפנים חדר

המחשב. נשק מתקדם היוצר פולס אלקטרומגנטי (EMP) יכול להשבית חדרי מחשב ברדיוס נרחב. טילים ורקטות יכולים להשבית חוות שרתים וריכוזי תקשורת. מתקפות של denial of service יכולות להשבית ארגונים שלמים.

בתקופה שלאחר מתקפת הטרור של 9/11 קבע הרגולטור האמריקאי שארגונים פיננסיים יידרשו לקיים אתר חלופי (DR) כ-500 מייל לפחות מחוות השרתים העיקרית. קביעה זו שונתה ל-30 מייל חיש מהר בשל מגבלות המרחק של התקשורת הסינכרונית באותם ימים. הדרישה למרחק רב לא הייתה מוטעית. 30 מייל לא יגנו על הארגון מפני אסונות טבע כגון רעידת אדמה או הוריקן או מפני פולס אלקטרומגנטי. בישראל המודעות לצורך במיגון מפני רעידות אדמה נמוכה מאוד למרות הסיכון העצום אך בשל המצב הביטחוני ואירועים כגון חומת מגן ועמוד ענן, המודעות לסיכון מפני טילים רקטות גבוהה מאוד.

השבתה של מרכזי מחשוב מרובים כתוצאה מרעידת אדמה יכול לגרום לפאניקה ולנזק רב למשק הלאומי. במקביל, ההסתברות של תקיפה פיזית על מרכזים פיננסיים ולאומיים גוברת והעלות לתוקף יורדת. כמנהיג הטכנולוגי של הארגון, מה על המנמ"ר לעשות?

- השבתת מרכזי מחשוב מרובים כתוצאה מרעידת אדמה יכולה לגרום לפאניקה ולנזק רב למשק הלאומי. במקביל, ההסתברות לתקיפה פיזית על מרכזים פיננסיים ולאומיים גוברת והעלות לתוקף יורדת. כמנהיג הטכנולוגי של הארגון, מה על המנמ"ר לעשות?

בחירה נבונה של אתר למרכז מחשוב חדש היא הדרך הזולה ביותר כדי לשלוט בסיכון הפיזי בעתיד. גם סכומי כסף ניכרים לא יחפו על הנזק שנגרם מבחירה גרועה של מיקום חוות שרתים. אתרי מרכזי מחשוב צריכים להיבחר על בסיס שירות, צפיפות סיבים, סיכונים טבעיים וסיכונים מעשה ידי אדם ועל ידי היכולת הפיזית לאבטחה היקפית וחיצונית.

לאחר בחירת המיקום, יש להקדיש תשומת לב לתכנון חוות השרתים ולמיגונה מפני איומי ייחוס שונים. קל מאוד היום להגן מפני רעידת אדמה על ידי בסיס סימטי המותקן מתחת לארונות ה-IT. סיכון אלקטרומגנטי בקירות מגן מפני האזנות ומפני הרס המערכות הנגרם מפולס אלקטרומגנטי. קירות בטון מזוין ומיזור נבון יגנו מפני פגיעת רקטות.

בארגונים נאורים, סמנכ"ל הטכנולוגיה (או המנמ"ר) ימצא שהמנכ"ל וסמנכ"ל הכספים תומכים בהקמת אתר גיבוי (או עיקרי) ממוגן. האתר החדש יכול להיות חסכוני מאוד באנרגיה ויכול לחסוך ממון רב בהוצאות התפעול עד כדי מיליוני שקלים בשנה לאתרים בינוניים.

ואם, רחמנא ליצלן, ימצא המנמ"ר שהנהלה מהססת לתמוך בהשקעה הדרושה, ישאל נא אותם מה לדעתם יקרה למחיר המניה של הארגון, אם חוות השרתים תושבת לשבועיים, או חודש, או חודשיים. אין לי ספק, שלאחר בחינת הנושא,

הוא ימצא בהם בעלי ברית חזקים ותומכים.

יגאל שניידר הוא מנכ"ל חברת אלכסנדר שניידר המתמחה בהקמת חוות שרתים. יגאל כותב בלוג מקצועי בנושא www.datacenter.org.il

