בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

בעניין: **מדינת ישראל**

ע"י משטרת ישראל - לשכת התביעות

ע"י ב"כ עו"ד עמוס כהן תובע

נ ג ד

מזרחי אבי

ע"י ב"כ עו"ד עמרי כבירי נאשם

הכרעת דין

מבוא

1. הנאשם, מר אבי מזרחי (להלן: "הנאשם"), הואשם בעבירה של נסיון חדירה לחומר מחשב בניגוד לסע' 4 לחוק המחשבים, תשנ"ה - 1995 (חדירה למחשבים) + סע' 34ד' לחוק העונשין, התשל"ז - 1977 (עבירת נסיון).

2. הטענה העובדתית בקליפת אגוז היתה כי ביום 22.9.02 בסמוך לשעה 19:25 ניסה הנאשם לחדור לאתר המוסד למודיעין ולתפקידים מיוחדים (להלן: "המוסד").[1]

החלטתי לזכות את הנאשם מכל אשמה.

3. היות ומדובר בשאלה משפטית המבוססת על רקע טכני לא פשוט הגעתי למסקנה כי לא יהיה מנוס מהסבר טכנולוגי, ולו בקצרה. אשר לכן, המשך הכרעת הדין יהיה לפי הפרקים הבאים.

- בתחילה נפרט בקצרה את האשמה ומהלך הדיון.

---

[1] אתר שכתובתו היא http://www.mohr.gov.il כל האתרים המופיעים בפסק הדין נחזו לאחרונה בתאריך 27.2.2004.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

- ניתן רקע טכני ארוך למדי שיבהיר עניינים שונים הקשורים למקרה שלפנינו. נשתדל במידת האפשר לקצר ובנקודות שנאריך יהיה זה משום שיהיה בהן צורך מאוחר יותר.
- ננתח את העבירה של חדירה למחשב ובמסגרתה נבדוק האם בדיקת אבטחת אתרים, מותרת או אסורה.
- נתאר עובדתית מה עשה הנאשם ולאור כך נגיע למסקנה הברורה כי הנאשם זכאי.

4. הדרך אכן היא ארוכה מהמקובל בפסקי דין פליליים רגילים, אך במקרה שלפנינו לא מצאתי ברירה אחרת.

<u>האשמה ומהלך הדיון</u>

5. בתאריך 19.6.03 הוגש כתב אישום נגד הנאשם ובו נטען כי הוא ניסה לחדור לחומר מחשב. הטענה העובדתית היא כי הנאשם התקשר לאתר האינטרנט של המוסד וניסה לחדור לתוכו אך זממו לא עלה בידו מכיוון שהאתר היה מוגן כדבעי.

6. ההקראה בתיק התקיימה ביום 14.9.03 והתקיימו בו מספר ישיבות הוכחות בתאריכים 9.10.03, 21.10.03 ו- 18.12.03.

7. כן הוגשו בהסכמה המסמכים הבאים:

ת/ 1 - הודעת הנאשם בחקירתו במשטרה מתאריך 19.2.03.
ת/ 2 - מסמכים מבזק ומחברת netvision המהווים את המסמכים על פיהם התברר מיהו הנאשם.
ת/ 3 - חשבונות טלפון לאחיו של הנאשם, מר קדם רונן, מראים את הטלפון ממנו נעשתה ההתחברות לאתר המוסד.
ת/ 4 - תדפיס מסונן של תוכנת snort.
ת/ 5 - תדפיסים מתוכנת ה- fire wall המגינה על אתר המוסד (כפי הנראה מכונת linux).

8. ההגנה הגישה את המסמכים הבאים:

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

נ/ 1 - הודעתו של המנהל הטכני של פרוייקט תהילה מר אריק וולף (להלן: "וולף" או "מומחה תהילה").

נ/ 2 - דו"ח פעולה.

נ/ 3 - חוו"ד מומחה מטעם ההגנה.

9. העידו העדים הבאים מטעם התביעה:

- עו"ד הגר רובין מהיחידה הארצית לחקירות הונאה (להלן: "השוטרת" או "רובין")
- פקד מאיר חיון, חוקר עבירות מחשב מהיחידה הארצית לחקירות הונאה (להלן: "השוטר" או "חיון").
- מר אריק וולף סגן מנהל פרויקט תהילה (להלן: "וולף").

10. מטעם ההגנה העידו העדים הבאים:

- הנאשם עצמו.
- מר צבי גרוס (להלן: "גרוס").
- מר גדי גיא (להלן: "מומחה ההגנה" או "גיא").
- עדת ההגנה גב' מיטל גיגי חברת הנאשם (להלן: "מיטל" או "החברה").

11. כמו כן, הוגשו בהסכמה תצהיריהם של מר אופיר ארקין מומחה לאבטחת מידע מטעם ההגנה וכן תצהירו של איש המוסד לעניין הירשמותו של מר אבי מזרחי כמועמד למוסד דרך אתר המוסד. שניהם גם נחקרו על תצהיריהם

12. הצדדים ביקשו לסכם בכתב והתיק הגיע חזרה לבית המשפט לאחר סיכומי ההגנה ותגובת המאשימה ביום 29.1.04.

13. כפי שציינו אין מנוס מרקע טכני לא קצר אך נזהיר מראש שמפאת קוצר היריעה ויתרנו פה ושם על הדיוק למען הבהירות.

<u>שיטת המנות, פרוטוקולים ופורטים</u>

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

14. בבסיס התקשורת ברשת האינטרנט עומדת שיטת המנות. כל שני מחשבים ברשת המבקשים להתקשר עושים זאת באמצעות פרוטוקול ייחודי. לכל מחשב המחובר לרשת האינטרנט בכל רגע נתון יש "כתובת" המורכבת מארבעה מספרים שבין 0 ל- 255. כל מחשב הרוצה להתקשר עם מחשב אחר על מנת לשלוח לו תקשורת כלשהי, עושה זאת על ידי שימוש בכתובת של המחשב האחר. המחשב השולח הודעות מחלק את הודעתו ל- "מנות" קטנות. כל מנה כזו מקבלת מספור ואליה מתלווה הכתובת הסופית.

15. נסביר זאת במילים פשוטות, אם מחשב A רוצה לשלוח הודעה למחשב B הרי בראש ובראשונה A מתקשר ל- B ואומר לו אני שולח לך הודעה בת נאמר 30 חלקים. כל חלק וחלק נשלח באופן נפרד אל הכתובת הסופית, כאשר אל כל חלק מוצמדת "תווית" שעליה מופיעים בקצרה הפרטים המשלימים. דהיינו, זוהי הודעה ממחשב A למחשב B ומספר המנה הזו הוא נאמר מספר 22 מתוך 30 המנות. המחשב B מקבל את המנות באופן נפרד, מסדר אותם לחבילה שלמה ובודק אם נעלמה בדרך מנה כלשהי. אם נעלמה המנה הוא שולח הודעה למחשב A ומבקש את המנה הזו ומנה זו נשלחת מחדש.

16. לשיטת המנות יש מספר יתרונות שאין להתעלם מהם הקשורות ליעילות השיטה. הדרך שעוברת כל מנה איננה דרך ישירה ממחשב A ל- B. המנה עוברת בדרך בין מחשבים רבים בהתאם לנתיב הפנוי באותה עת. כל מחשב הנמצא בתווך המקבל את המנה מכיוון A ושולח אותה לכיוון המחשב B, צריך זמן לקבל את המנה ולשולחה. אם המנה קטנה יכולים המחשבים להשתמש ולשלוח מספר מנות רב יותר באותו פרק זמן ולעבוד יחדיו. תכונה חשובה אולי אף יותר, היא העובדה שאם ישנה תקלה במנה אחת, אין צורך לשלוח מחדש את כל ההודעה. נסתכל לדוגמא על פקס. אם ישנה תקלה בפקס יש לשלוח את כל הודעת הפקס מחדש. כשמדובר במנות, די לשלוח מחדש את המנה החסרה.

17. צריך כמובן שהמחשבים ידעו לדבר זה עם זה. כלומר, אם מחשב B מקבל מנה כלשהי שאליה מצורף הסבר על טיבה של המנה הוא צריך לדעת לקרוא זאת. לצורך כך, פותחו ברשת פרוטוקולים שונים ורבים על מנת שכל מחשב ידע ויבין את פשר המנות השונות הנשלחות אליו.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

בבסיס האינטרנט עומד פרוטוקול המכונה TCP/IP.[2] פרוטוקול זה מאפשר לכל מחשב להבין מהיכן נשלחה אליו המנה ומה טיבה.[3]

18. כפי שציינו, לכל מחשב המחובר ברגע נתון לאינטרנט יש מספר ייחודי. אולם, גם אם מחשב מקבל הודעה כלשהי הרי במחשבים רבים ישנם תהליכים מקבילים. כך למשל, כל מחשב ביתי משתמש באינטרנט לגלישה, אך גם לשליחה וקבלה של דואר אלקטרוני, לעיתים להורדת מידע באמצעים שונים וכן הלאה. איך ידע כל מחשב לאן לשייך את ההודעה או "המנה" שהוא מקבל ממחשב אחר?

19. לכל מחשב יש מה שמכונה "פורטים" אשר מטפלים בתהליכים שונים. ישנם פורטים רבים כאלו ומערכת ההפעלה של המחשב עוברת מפורט לפורט כל הזמן ובודקת האם קיבלה הודעה כלשהי, או בקשה כלשהי מפורט מסויים. פורט שכזה שניתן לפעול בו נקרא פורט "פתוח".[4]

20. כדי להקל על כתיבת תוכניות חדשות ועל שיתוף הפעולה בין המחשבים יש לפורטים הללו מספרים מוסכמים מראש. פורט 80 למשל משרת בדרך קבע את הדפדפנים השונים לצורך גלישה באינטרנט, פורט 25 מוקצה לשליחת דואר אלקטרוני, פורט 110 לקבלת דואר אלקטרוני, וכן הלאה.

<u>שמות, מספרים, הקצאות, וגלישה באינטרנט</u>

21. כפי שהסברנו, לכל מחשב המחובר ברגע נתון לרשת ישנו מספר ייחודי. אולם הציבור הגולש איננו מכיר כלל מספרים אלו אלא מכיר בעיקר שמות אתרים. לדוג' אתר בית המשפט הוא www.court.gov.il . להיכן נעלם המספר?

---

[2] **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol

[3] למען הדיוק הטכני הרי קיים גם פרוטקול בשם UDP. אין בו תהליך של הקמת קשר ובדיקה אם החומר נשלח ליעד, ואין כל בקרת עומס או זרימה. בפרוטוקול זה המידע פשוט נשלח. יתרונו הוא במהירות ובמחיר.

[4] לצורך הבהירות נקטנו בהגדרה פשטנית במקצת. בפועל ישנם פורטים הידועים לכולם (והגישה אליהם אמורה להיות מבוקרת), יש פורטים רשומים, וישנם פורטים דינמיים. פרטים עליהם ניתן למצוא באתר: http://www.iana.org/assignments/port-numbers

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

22. התשובה היא שכבר בשלב התפתחות מוקדם של רשת האינטרנט התברר כי קל הרבה יותר לזכור שמות מאשר 4 מספרים אקראיים. לצורך כך קיימים מספר "שרתי שמות" (שרת פה כמו בכל מקום משמעותו היא מחשב שתפקידו לתת שירות).[5] כאשר אנו מקישים את שם האתר שאליו ברצוננו לגלוש ישנם שרתי שמות שאליהם שולח המחשב שלנו את כתובת האתר והם מחזירים לו את המספר. אשר על כן, ישנו מעין "תרגום" של השמות הידועים למספרים. כך למשל מספרו של אתר המוסד הוא 147.237.72.43, ושל אתר בית המשפט 10.1.1.48

23. את המספרים הייחודיים לכל מחשב ואת השמות של האתרים מקצה גוף בשם ICANN.[6] יש לזכור שהמספרים הללו אינם תמיד קבועים. כך למשל, כל ספק אינטרנט מקבל מלאי כלשהו של מספרים. כאשר אחד המנויים מתחבר אל הספק הוא מקבל באופן זמני את אחד המספרים המוקצים לספק האינטרנט שלו ומספר זה משמש אותו במשך גלישתו. כאשר הוא מתנתק מהספק הופך מספר זה להיות חופשי ומשתמש אחר שמתחבר דרך הספק מקבל את המספר שהתפנה. בניגוד למשתמשים ביתיים, הרי לשרתים מוקצה כתובת קבועה. זאת משום שלשרתים אלו ניגשים הרבה יותר וכתובת קבועה תחסוך רבות.

24. נסביר כעת ברפרוף מה עושים אנו כאשר אנו גולשים באתר מסוים. עם התחברותנו לאתר, הרי המחשב שלנו שולח הודעה למחשב שמכיל את האתר (המכונה שרת האינטרנט או שרת האתר). כל שמבקש המחשב שלנו באמצעות פרוטוקול ידוע משרת האתר הוא לשלוח לו אינפורמציה. את האינפורמציה הזו שנשלחת גם היא בצורת מנות מפעיל הדפדפן שלנו על המסך וכך אנו רואים את האתר. במילים אחרות, אין "מקום" או "אתר" פיזי שאליו אנו נכנסים. כל שיש הוא אינטראקציה בין המחשב שלנו לבין שרת האתר השולח אלינו את החומר אותו אנו מבקשים.

<u>העקרונות התיאורטיים של רשת האינטרנט</u>

---

[5] הללו מכונים: DNS - Domain Name System

[6] Internet Corporation For Assigned Names and Numbers. זהו גוף בינלאומי הפועל ללא מטרת רווח שכתובתו באינטרנט היא: http://www.icann.org

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

25. ממה שהוסבר קודם לכן, ברור שכדי שרשת האינטרנט תפעל יש צורך בהסכמות רבות. אולם, לתיאורטיקנים של הרשת בתחילתה היו דרישות רבות אף יותר. הם ראו את רשת האינטרנט כאם כל רשתות המחשבים שבעולם. רשת שאליה יוכל להתקשר כל מחשב או ליתר דיוק כל רשת מחשבים (להלן נתייחס למחשב או לרשת אם כי ברוב המקרים המחוברים לאינטרנט הם רשתות).

26. אותם מייסדי הרשת ביקשו לקבוע כמה כללים עקרוניים.

27. ראשית, כל רשת המחוברת לאינטרנט תוכל להתקשר לאינטרנט ולכל רשת מחשבים אחרת מבלי צורך לשנות כל דבר בה. דהיינו, כל רשת מחשבים בעולם או כל מחשב גדול לצורך זה יוכל להתקשר דרך האינטרנט.

28. שנית, העברת המידע באינטרנט צריכה להיות על בסיס של יעילות מירבית. אם מנה לא הצליחה להגיע ליעדה הסופי זמן קצר אחרי זה יודע על כך למקור ותישלח הודעה נוספת. זאת, כדי להבטיח את התקשורת לאינטרנט.

29. שלישית, "קופסאות שחורות" יהיו הכלים העיקריים לחיבור בין הרשתות. אותן קופסאות שחורות יקבלו מידע ויעבירו אותו הלאה עד להגעה לכתובת המבוקשת ללא מגע באינפורמציה וללא כל ידיעה על תוכנה. במילים אחרות, אם מחשב א' שולח הודעה למחשב ב' דרך רשת של מחשבים באמצע, הרי כל מחשב שבדרך לא יטרח כלל לקרוא את ההודעה. אותו מחשב מתווך יקבל את המנה, יבדוק לאן צריך לשלוח אותה הלאה וישלח אותה הלאה מבלי להתעסק בה יתר על המידה. אגב, אותן קופסאות שחורות הן אלה שהפכו ל- gateways routers.

30. רביעית, ואולי חשוב מכל, העקרון היה שלא יהיה כל בקרה מרכזית או דרך לשליטה כלשהי על רשת האינטרנט. דהיינו, רשתות המחשבים תוכלנה להתקשר אחת לשניה בלא שום אפשרות של מאן דהוא לשלוט על התוצאה הסופית.[7]

---

[7] על עקרונות אלו ועל ההיסטוריה של האינטרנט בכללותה ראו:
http://www.isoc.org/internet/history/brief.shtml

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

31. יושם לב, שעקרונות אלה של רשת האינטרנט דורשים הסכמה רבה בין כל הרשתות והמחשבים המשתמשים. אולם, לאחר שנוצרה הסכמה זו הרי רשת האינטרנט הפכה ליציבה למדי וקשה לפגוע בה.

<u>חורי האבטחה, קירות אש ותוכנות אבטחה</u>

32. נקודה בולטת שעליה לא חשבו ראשוני הרשת היא שאלת הביטחון. רשת האינטרנט הוקמה ותוחזקה על בסיס רעיונותיהם של מדענים ללא כל מחשבה על שימושיה הכלכליים. הללו ראו ברשת משאב משותף לכלל הציבור ועל סמך כן בנו את רכיביה. המחשבה של אבטחה, בטחון, ואפשרויות לניצול לרעה לא עמדו בראשית מעייניהם של אותם מהנדסים ומומחי מחשב. הדבר מתברר כשרואים כמה מן התקלות והבעיות שניתנות להיגרם על ידי אדם ונסביר כמה מהן הרלוונטיות יותר לענייננו.

33. כפי שאמרנו, כל מחשב מקבל "מנות" ומחבר אותן להודעות שלמות. אולם, מה קורה כאשר מחשב מקבל מנות בקצב בו איננו יכול לטפל? כמובן, יש לכל מחשב מעין "מחסנית" (Buffer) שבה הוא יכול לאחסן את המנות הממתינות לטיפול. אולם, מה יקרה אם יצטברו יותר מנות מתחולת המחסנית? אם לדוג' יכול מחשב לטפל ב- 4,000 מנות כל שניה מה יקרה אם יישלחו אליו 20,000 מנות בשניה? התשובה היא שבמקרה כזה המנות הנותרות יאבדו ללא טיפול וייעלמו. תיאורטית כמובן, המחשב השולח יקבל הודעה כי עליו לשלוח את המנה מחדש אך אם יהיה עומס גם היא תאבד ותישאר ללא טיפול. בבסיס עקרון זה, עומדת אחת ההתקפות הידועות ביותר ברשת האינטרנט המכונה DOS (Denial of Service).[8]

34. שרת של אתר אינטרנט אינו יכול לשרת יותר מאשר כמות מוגבלת של משתמשים. אם לדוג' ינסו להתחבר 100,000 איש בבת אחת לשרת של אתר בתי המשפט סביר להניח שרובם לא יוכלו להתקשר אליו כלל. נשים לב מה יקרה. נניח ששרת אתר כלשהו יכול לקבל 4,000 פניות בכל רגע נתון. אם ברגע נתון יקבל פתאום 100,000 פניות שירות הרי 96,000 מהם לא יוכלו לקבל שירות. יתירה מכך, אפילו אם ימתינו אותם 96,000 "בתור" לקבל שירות גם אז לא יזכו לקבל

[8] אין זה המקום להסביר את הרקע הטכני, אולם לעיתים התקפה של המחשב בעודף מידע (buffer overflow) איננה אלא רק שלב ראשון בהשתלטות על המחשב.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

שירות. זאת משום שכל הדפדפנים ותוכנות הגלישה מכוונים להמתין פרק זמן מסוים ואם אינם מקבלים את השירות באותו פרק זמן הם חוזרים למחשב השולח ומודיעים כי הפעולה נכשלה.

35. נחזור שוב לעניין שהצגנו של ההתקפה על מחשב. אם ברצון מזיק כלשהו לתקוף אתר כל שהוא צריך הוא לשלוח לאותו אתר מספר גדול של בקשות שירות מעבר ליכולת האתר לספק. אחת השיטות למשלוח מספר עצום ורב של בקשות שירות הוא להשתלט על מספר רב של מחשבים "ולתכנתם" כך שבאותה שעה ובאותו זמן כולם גם יחד יחלו לשלוח הודעות שירות ברצף לשרת שאותו מבקשים הם "להפיל".

36. כמובן, כנגד כל התקפה יש הגנה ולהיפך. השרתים הגדולים מתוכנתים כך שבמידה ויקבלו מספר בלתי סביר של בקשות שירות מכתובת מסוימת הם יחסמו את אותה כתובת ויתעלמו מכל המנות המגיעות אליהם משם.

37. אולם, מטבע הדברים קיימים "חורי אבטחה" רבים. כפי שציינו מקודם, רשת האינטרנט מורכבת מהמוני שרתים שונים, רשתות שונות, אפליקציות שונות, תוכנות שונות ועוד ועוד. חור/פגם אבטחה לעניינו, הוא מצב שבו אדם עם נטיות להזיק יוכל לנצל אפשרות כדי לגרום נזק למחשבים שונים. פגמים כאלו ימצאו כמעט בכל מערכת מחשבים. אולם ברור כי חור שניתן לנצלו במערכת Linux לדוגמא איננו בהכרח ניתן לניצול במערכת חלונות. פגם בתוכנת דואר אחת לא יהווה פגם בתוכנות דואר מסוג אחר וכן הלאה וכן הלאה. בכל מקרה, מספרי חורי האבטחה הללו הוא עצום ורב. רק ב - Windows (על גרסותיה השונות) התגלו 119 פגמי אבטחה בשנת 2003 לבדה.

<u>קירות אש, ותוכנות פסיביות ואקטיביות לבדיקת אבטחה</u>

38. כדי להימנע מהתקפות שונות ומניצול פרצות פותחו אמצעים שונים. העיקריים שבהם הנם חומות האש ותוכנות לבדיקת אבטחה. מה שמכונה "חומת אש" (Fire Wall) הנה תוכנת אבטחה הנמצאת בדרך כלל בין הרשת המאובטחת לבין האינטרנט. תפקידה של החומה הוא לנטר את המנות הנכנסות ולסרב לקבל מנות אחרות, והכל בהתאם למדיניות מנהל האבטחה ברשת. מדובר בהגנה תוקפנית במקצת ולא בהכרח מתוחכמת. יכול למשל מנהל רשת להחליט כי

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

ברשת שלו לא יתקבל כל דואר אלקטרוני. הדרך לכך פשוטה. כל מנה שמיועדת לפורט 110 פשוט לא תתקבל, הרשת תסלק אותה ותתעלם ממנה.

39. אולם, גם בחומת האש אין די משום שייתכן ומנות "לגיטימיות" יוכנסו לרשת אך עם כניסתם לרשת ייגרמו נזקים. מספר תוכנות מטפלות בכך. הללו, מנסות לזהות תבניות שונות בהתנהגות המנות ובהתנהגות המחשבים (ליתר דיוק, הכתובות) ששולחות בקשות למחשב. התקנים אלו הן בדרך כלל תוכנות פאסיביות הנמצאות ברקע ומטרתן להזהיר את האחראים על האבטחה כי ייתכן וישנה איזו שהיא התקפה או "פעילות חשודה" ברשת.

40. המפורסמת מבין תוכנות האיתור הללו היא תוכנת snort שהיא תוכנה חינמית בעלת קוד פתוח. דהיינו, מדובר בקהילת מתכנתים מכל העולם העוזרים אחד לשני חינם אינם כסף כדי לשכלל את התוכנה ולפתור בעיות הקיימות בה.[9]

41. תוכנת ה- snort היא תוכנה שמטרתה היא זיהוי התקפות או חדירות. בניגוד ל- fire wall (חומת אש) שתפקידו הוא לעצור התקפות כאלה מן הרשת. הדגש בתוכנת ה- snort, הוא זיהוי ולא עצירה. יש כאלה שממקמים אותה מחוץ לרשת לפני חומת האש על מנת לזהות את ההתקפות עוד בראשיתן כולל כאלה שלא הצליחו, ויש כאלו שממקמים אותה אחרי חומת האש למקרה שתהיה חדירה לרשת.[10] המהדרים כמובן ממקמים אותן גם לפני וגם אחרי חומות האש למיניהן.

42. לחומות האש ולתוכנות הפסיביות יש להוסיף תוכנות אקטיביות לבדיקת כשלי אבטחה למיניהם. כיצד יכול בעל אתר לדעת שאתרו מאובטח? באופן תיאורטי התשובה לכך פשוטה. הוא צריך לעבור על הרשימה הידועה של כשלי אבטחה שהתגלו עד להווה ולבדוק חור חור כשל כשל האם הוא נמצא במחשבו אם לאו. במידה ונמצא כי קיים כשל במחשבו הוא צריך להחליט אם לטפל בו וכיצד. אולם, השלב הראשוני הוא בדיקת כל אפשרויות אלה.[11]

---

[9] ניתן לראות את ה- snort באתר www.snort.org.

[10] תועלת נוספת במיקום תוכנת ה- snort אחרי חומת האש היא זיהוי תבניות לא לגיטימיות של משתמשים חוקיים ברשת. במילים אחרות, ניתן לעקוב גם אחרי התנהגויות סוררות של משתמשים חוקיים.

[11] תוכנות לבדיקת אבטחה צריכות לזהות אלו שירותים ותהליכים מבצע השרת, ואחר כך האם ניתן לבצע מניפולציות על אותם שירותים באמצעות חורי אבטחה. לצורך כך הן בודקות בראשונה אלו פורטים "פתוחים" במחשב. זאת כדי לזהות אלו שירותים מספק השרת ועל כן הפורטים הקשורים לשירותים אלו יהיו

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

43. אלא, שחורי אבטחה במחשבים הם דבר דינמי ומשתנה. כל חברה המכבדת את עצמה המוצאת כשל אבטחה במוצריה מיד שולחת תיקון ללקוחותיה. כך למשל microsoft שולחת באופן קבוע ומציבה על האתר שלה טלאי אבטחה לחורים שהתגלו. יתירה מזו, ישנן תוכנות רבות, מחשבים שונים, מערכות הפעלה נדירות, ועוד. תוכנית שתכלול את כל החורים שהתגלו אי פעם איננה מעשית.

44. בפועל, ישנן תוכנות חינמיות (ללא תשלום) ותוכנות מסחריות. בדרך כלל התוכנות המסחריות הן יעילות יותר מתוכנה חינמית. צריך להבין שכדי שתוכנית לבדיקת כשלי אבטחה תהיה יעילה, היא צריכה להתעדכן באופן קבוע, ליתר דיוק, מדי יום ביומו ולפעמים יותר מפעם ביום. היא צריכה כל פעם להוסיף פרטים ולהוריד פרטים לבדוק מערכות שונות על פלטפורמות שונות וכן הלאה. משימה כזו של עדכון היא קשה בדרך כלל. כיום, אין תוכנות חינמיות מובילות להוציא תוכנה בשם nesus שגם היא מתעדכנת מפעם לפעם על ידי קהילת מתכנתים שעושים זאת חינם אין כסף.

45. לעומת זאת, קיימות תוכנות מסחריות יקרות ברמה של עד עשרות אלפי דולרים העושות בדיקות מסוג זה שהזכרנו. מקובל לטעון שהתוכנות המסחריות הן טובות יותר הן מבחינת האבטחה והן מבחינת הבדיקה. דהיינו, הן בודקות את הכשלים עד לרמת לחיצת המקש האחרונה (דהיינו, הן מגיעות עם הבודק עד השלב שבו ניתן לגרום נזק אם אכן היה הבודק מעונין לעשות כן). למרות המחירים הגבוהים הרי ישנם אתרים כגון אתרי מסחר ובנקים שבשבילם הוצאות כאלה תהיינה כדאיות ואפילו הכרחיות.

46. צריך לזכור שאלו גם אלו, הן רק תוכנות לבדיקת כשל אבטחה. לשם שימוש בכשל הזה לשם התקפה על אתר יש צורך בידע מקיף הרבה יותר. אם נשתמש במטאפורה (לא מוצלחת במיוחד), העובדה שכל אחד רואה דרך חלון מכונית אם יש אזעקה אם לאוו, איננה מספיקה לפריצתה משום שצריך לדעת כיצד לפרוץ את מנעוליה ולהניע ללא מפתח.

"פתוחים". אשר על כן הן מתחילות בדרך כלל בבדיקת הפורטים, מה שמכונה - Port Scanning. במשפט האמריקאי מתייחסים לכן פעמים רבות ל – Port Scanning

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

47. ניתן דוגמא אחת הרלוונטית לענייננו. כפי שהסברנו קיימים בכל מחשב פורטים רבים המזוהים עם תוכניות ותהליכים בו. אולם, כיצד יגיב מחשב אם יקבל מנה המיועדת לפורט שאיננו קיים כלל? ובדרך כלל מדובר על פורט מספר 0 שאין לו תפקיד ואיננו קיים. יתכן כי המערכת פשוט תתעלם ממנו לחלוטין, אך יתכן גם שהמערכת תבזבז זמן בנסיון לבדוק מה לעשות עם מנה זו. היו גם מערכות שבזבזו זמן רב כדי לברר מה לעשות עם המנה, זמן שגדל עם מספר המנות. דהיינו, אם למנה הראשונה שנשלחה לכתובת הלא נכונה בזבז המחשב חצי שניה כדי לבדוק מה לעשות עימה, הרי כשנשלחו 100 מנות הרי בזבז לא 100 X חצי שניה אלא 100 X שניה. דהיינו, ככל שישלחו יותר מנות לפורט שאיננו קיים יגרום הדבר למערכת להתבלבל עד לקריסתה.

48. מבחינה תיאורטית יש פה מעין כשל אבטחה אלא שפרקטית יהיה זה רק השלב הראשון בדרך לניצול חור שכזה. שכן, גם אם יודעים אנו שניתן לנצל כשל זה, צריך עדיין לגרום לכך שמספר מחשבים ישלחו מספר עצום של הודעות לפורט 0 (קנה המידה הוא מיליונים ומליארדים). אם לא ישלחו הודעות מעין אלו, הרי גם אם יש כשל לא ניתן להשתמש בו.

49. יש לזכור שגם אם כשל זה קיים, ישנם בעלי אתרים רבים שלא יטרחו לתקנו. אם מדובר באתר של תלמיד תיכון המפאר את עצמו והמציג מספר תמונות של בני משפחתו, למה שיתאמץ לחתום זאת? מבחינתו אם מישהו רוצה להתאמץ עד כדי כך ולגרום לקריסת האתר לפרק זמן כלשהו יש בכך מחמאה. הוא בוודאי לא יטרח להשקיע בקניית חומות אש ו/או תוכנות הגנה למיניהן. בין השאר מהסיבה שתוכנות ואמצעים בתחום אבטחת מידע אינם דבר זול. לא כל בעל אתר/שרת יכול להרשות לעצמו להצטייד בציוד זה.

50. דוגמא זו אופיינית לרוב כשלי האבטחה. גם אם קיימת אפשרות לגרום לאתר נזק, יהיו רבים שלא יטרחו לנסות לחסום זאת. מבחינתם גם אם יגרם נזק הרי מדובר תמיד על נזק זמני. וגם אם ייהרס האתר כליל יבנו אותו מחדש. צריך לזכור שוב, שככל שאנו מתכוונים במילה "אתר" איננה אלא מחשב, לאו דווקא חדש או חזק במיוחד, המחובר לכמה קווים וכתגובה לאנשים שמבקשים ממנו אינפורמציה שולח אותה אליהם. בדרך כלל, הנזק המקסימלי בעת קריסה טוטאלית הוא שיחזור מגיבוי.

ואחרי הרקע הלא קצר, נעבור לבסיס המשפטי.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

הרקע המשפטי - עבירת החדירה למחשב במשפט הישראלי

51. הנאשם הואשם בעבירה על סעיף 4 לחוק המחשבים התשנ"ה - 1995. סעיף זה מופיע בפרק ב' הדן בעבירות מחשב ונוסחו הוא:

4. החודר שלא כדין לחומר מחשב הנמצא במחשב, דינו - מאסר שלוש שנים; לעניין זה, "חדירה לחומר מחשב" - חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו, אך למעט חדירה לחומר מחשב שהיא האזנה לפי חוק האזנת סתר, התשל"ט-1979.

חומר מחשב לעניין חוק המחשבים מוגדר בסעיף 1 לחוק שהוא סעיף ההגדרות ועל פיו:

"חומר מחשב" - תוכנה או מידע;

תוכנה מוגדרת גם היא בסעיף ההגדרות בזו הלשון:

""תוכנה" - קבוצת הוראות המובעות בשפה קריאת מחשב, המסוגלת לגרום לתיפקוד של מחשב או לביצוע פעולה על ידי מחשב, והיא מגולמת, מוטבעת או מסומנת במכשיר או בחפץ, באמצעים אלקטרוניים, אלקטרומגנטיים, אלקטרוכימיים, אלקטרואופטיים או באמצעים אחרים, או שהיא טבועה או אחודה עם המחשב באופן כלשהו או שהיא נפרדת ממנו, והכל אם אינה מיועדת לשימוש במחשב עזר בלבד."

הבעייתיות בהגדרת המונחים "חדירה" ו – "שלא כדין"

52. אין הגדרה מספקת לחדירה למחשב. עצם המושג "חדירה" הוא מושג הכרוך בעולם הגופני שבו יש לדברים נפח ומשקל. חדירה בעולם הפיזי פירושה מעבר גבול/גדר/קיר/מחסום ו/או כל תחום מוחשי אחר. כדי לחדור צריך שיהיו גבולות אותם צריך לעקוף ולעבור. אולם למה הכוונה חדירה כשמדובר במחשב?

53. הסעיף אכן מגדיר **"חדירה לחומר מחשב" - כחדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו.** אולם אין כל ביאור בהיר ל"חדירה". המונח "חדירה" מוגדר באמצעות

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

המילה חדירה כך שההגדרה איננה מקדמת אותנו. האם כל התקשרות למחשב היא חדירה? האם כל שיח אינטראקטיבי בין מחשב א' למחשב ב' מהווה חדירה של א' ל-ב? מהם אותם גבולות שצריך לעבור כדי לחדור?

54. וכמובן זהו רק השלב הראשון, שכן לא כל חדירה אסורה אלא רק חדירה שלא כדין. גם אחרי שנצליח להגדיר חדירה בדרך זו או אחרת, נשאלת השאלה מהו המונח שלא כדין? האם בכל מקרה שבו לא רצה בעל האתר בהתקשרות כזו מדובר בחדירה שלא כדין? האם די בחדירה שנעשתה שלא בהתאם לחוזה (מפורט או מכללא) בין החודר לבעל המחשב הנחדר כדי תחשב שלא כדין? האם ניתן כלל להתייחס לנורמות אזרחיות הסכמיות? האם כדי שתהיה חדירה כדין צריך אישור מפורש לחדור? ועוד ועוד.

<u>הגישות בעולם ובישראל בנוגע לעבירת החדירה</u>

55. כפי שציין ב"כ התביעה בסיכומיו המאלפים, הרי ניתן כיום לראות בעולם שתי גישות לגבי שאלת החדירה למחשב. הגישה האמריקאית היא צרה יותר ומתירה יותר את ה - "דו-שיח החופשי" בין מחשבים באינטרנט. הפסיקה והחוק האמריקאים מתירים עקרונית מעין חדירה והיא אסורה אך ורק אם היא מלווה בשימוש לא מורשה או גרימת נזק למחשב. יתירה מזו, במשפט האמריקאי יש צורך גם בכוונה לעבור עבירה וגם בכך יש הרחבה.[12] הגישה האירופאית 3(ואליה מצטרפות ארצות אחרות) היא רחבה יותר. על פיה עצם החדירה למחשב אסורה בלא קשר לגרימת נזק כלשהי.

56. אני מסכים עם ב"כ התביעה כי פרשנות סבירה של הסעיף הישראלי מלמדת כי עצם החדירה למחשב אסורה. לשון החוק היא ברורה וחד משמעית ועל פיה עצם החדירה אסורה. בית משפט זה בעניין אחר קבע במפורש כי מחיקת חומר מחשב אסורה מבלי קשר לשאלת גרימת

[12] גם במשפט האמריקאי חל שינוי לאחרונה עקב התקפות הטרור של ה - 11 בספטמבר וחוקים שחוקקו בעקבותיה. אולם אין זה המקום לעמוד על כך.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

הנזק.[13] ובדרך ההיקש ניתן ללמוד ממחיקה לחדירה. ברור כי במשפט הישראלי אין צורך כי החדירה תהיה מלווה בנזק כלשהו. אבל מה היא חדירה?

57. גם באירופה שאליה מבקש ב"כ התביעה להידמות, יש אסכולות שונות. יש המבקשים להגדיר חדירה רק במקרה שבו החודר עבר מערכת הגנה כלשהי. החוק הנורווגי למשל מדבר על: "breaking a protective device", החוק הפולני מדבר על "special protection for that information", החוק ההולנדי מדבר על "Breaks through a security system", החוק האיטלקי מדבר על protected by security measures, ועוד כהנה וכהנה.[14] החוק הישראלי לא מדבר על כך בפירוש והגדרת החדירה בו איננו ברורה.

58. אולם לא זוהי השאלה שלפנינו. השאלה שלפנינו היא האם בדיקת אבטחתו של אתר מותרת אם לאוו? האם זוהי פעולה רצויה וחוקית או לכל הפחות לא אסורה, או שמא עצם הבדיקה מהווה ניסיון אסור לחדור כדברי התביעה?

<u>הבעייתיות הכללית בעבירה של חדירה למחשב</u>

59. כפי שטען לאחרונה ממש המלומד Kerr (להלן: קר) הרי ישנה אי בהירות בהגדרה המשפטית של המונח חדירה למחשב.[15] פרופ' קר תמה במאמרו על כך שאין כמעט מדינה שלא חוקקה חוקים האוסרים חדירה שלא כדין למחשב, אך עד היום אין קונצפציה ברורה לשאלה מהי אותה חדירה שלא כדין ומהם מאפייניה הבולטים. פרופ' קר הציע לכן הצעה מעניינת המבוססת במקצת על הסיבות לחקיקת רוב חוקי המחשבים כיום.

60. חוק המחשבים חוקק בתקופה בה הייתה סביבת העבודה שונה. בתקופה הטרום-אינטרנטית ואף מעט אחריה, כל התקשרות עם מחשב הייתה באמצעות הכנסת שם משתמש כלשהו שגובה בסיסמת כניסה. כדי להתחבר היה צורך להתקשר, להזין שם וסיסמא ואז ורק אז

---

[13] ת"פ 3813/99 מדינת ישראל נ. עודד רפאלי, דינים שלום, כרך טז' עמ' 861.

[14] החוקים במדינות רבות ותרגומיהם לאנגלית מופיעים באתר:
http://www.mosstingrett.no/info/legal.html

[15] Orin S. Kerr "Cybercrime's scope: Interpreting "access" and "Authorization" in computer misuse statuter" New York University Law Review (November 2003) Vol. 78 No. 5 pp. 1596-1668.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

הופעל החיבור. בתקופה זו, היה ברור מהי חדירה. חדירה הייתה בעצם עקיפה של הצורך בשם וסיסמא, בדרך כלל, על ידי שימוש בשמות וסיסמאות של אחרים. לא היה לכן כל צורך מיוחד להסביר את המונח חדירה.

61. המצב הטכנולוגי כיום שונה בהרבה. מחשבים מקושרים ומתקשרים ביניהם כיום בדרכים משונות. דואר אלקטרוני, החלפת תכנים אוטומטית, קבצי מוזיקה המוצעים לכל, שידורי רדיו וטלוויזיה דרך האינטרנט, מצלמות רשת בזמן חי, ויישומים שונים ורבים אחרים זמינים לשימוש. חלקם אף פועלים באופן אוטומטי כמעט ובשקוף למשתמש. במצב מעין זה של פעילות מתמדת, רוחשת, ושוקקת, לא ברור תמיד מהי חדירה מותרת, מהי חדירה חצופה, ומהי חדירה שלא כדין.

62. לדעת פרופ' קר מוגדר כיום המונח חדירה שלא כדין בצורה אינטואיטיבית מדי. לדעתו יש להרחיב את המונח "חדירה למחשב" ולכלול בתוכו כל תקשורת אינטראקטיבית בין מחשבים שונים. לשיטתו, במצב הקיים כיום של אינטראקציה בין מחשבים, הרי החדירה קיימת כמעט תמיד ואת ההבדל בין חדירה מותרת לאסורה יש למצוא ביסוד של "שלא כדין". הצעתו היא להבדיל בין חדירות "שלא כדין" הנובעות מיחסים חוזיים שבין הצדדים לבין חדירות שעקפו סיסמאות והגנות המבוססות על קוד המחשב (ובביטויו Regulation by Code Versus Regulation by Contract).

63. לגישתו, עצם העובדה שבעל מחשב איננו שש למעשי החודר אליו, איננה מספקת. העובדה שבעל האתר איננו מעוניין במעשי אחרים אין לה דבר עם ההליך הפלילי. רק אם החדירה הצליחה לעקוף אמצעי אבטחה ברורים כלשהם, ומטרתה הייתה לעקוף אמצעים אלו, אז ורק אז מדובר בחדירה שלא כדין.

64. על תפיסתו ניתן להתווכח, ובמיוחד על הצעתו לוותר על אלמנט החדירה כליל ולהתרכז בשאלת חוקיות המעשה ("כדין" או "לא כדין"? זוהי השאלה לגישתו). אולם זוהי עוד הוכחה לבעייתיות המושג חדירה.

<u>על הבעיה בתפיסת האתר כ"מקום" שניתן לחדור אליו, ועל היקשים מהחוק הפלילי הרגיל</u>

בתי המשפט

בית משפט השלום ירושלים | | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | | תאריך: 29.2.2004

65. ישנה ביקורת קשה בעולם המשפטי על עצם המטאפורה של האתר כמקום. ישנם מלומדים הטוענים שהמושג cyberspace לכשעצמו שגוי וגורם נזק. העובדה שאנו רואים את האינטרנט כמקום שניתן לחדור אליו גורמת לכך שאנו משליכים עליו את הנחותינו מהעולם המוחשי. אשר לכן התחלנו לראות את האינטרנט כמרחב שבו לכל אתר ואתר ישנו מקום פרטי משלו השייך רק לו. זאת בניגוד גמור לדרך שבה נבנה האינטרנט כשייך לקהילה כולה וללא בעלות פרטית או שליטה על משאביו.

66. הבולט במבקרים אלו הוא Dan Hunter.[16] לטענתו, דימויים שגויים אלו גורמים למה שהוא מכנה התנועה לסגירת הרשת (Cyber Enclosure Movement). עצם התפיסה של האינטרנט כמקום גורמת לנו להתייחס אליו כמו מקום בעולם הפיזי, ולנסות לחלק אותו לנתחים הנמצאים בבעלות פרטית כשמטרת הבעלים היא רווח בעיקרה. אולם לטענת Hunter מגמה זו סותרת לחלוטין את העקרונות עליהם נבנתה רשת האינטרנט. הרשת בנוייה ממחשבים המחליפים "מנות" אינפורמציה ושולחים מנות כאלו ממחשב למחשב באופן וולנטרי. הרשת נבנתה ממאות ואלפי מהנדסים ומדענים שללא תמורה ושכר ולשם שמים בלבד יצרו פרוטוקולים ושיתפו פעולה למען הצלחתה. מגמה זו גם ממשיכה חלקית כיום. ישנם אתרים רבים ברשת שבעליהם העלו עליהם חומר רב אותו הם מציגים לראווה לכל דיכפין וזאת אך ורק לטובת הטוב הכללי. מידע חופשי זה הוא רב ומגוון. החל מאלפי יצירות ספרות נגישות לכל בפרויקט גוטנברג,[17] ועד למפות עתיקות של ירושלים,[18] ועוד עשרות אלפי אתרים הקיימים אך ורק בהתנדבות וללא תמורה. על פי Hunter, התנועה לסגירת הרשת יכולה לגרום לכך שמשאבים ציבוריים שכיום הם מובנים מאליו יסגרו היות וכלכלית לא יהיה זה רווחי לשום אדם פרטי להחזיקם.

67. אין זה המקום להיכנס לבחינת תיאוריה זו. אולם לענייננו חשוב להבין כי ישנה ביקורת מוצדקת על ההיקשים המשפטיים שנעשים מחוקים פליליים רגילים המתייחסים לעולם הפיזי, למעשים בעולם האינטרנט. גם אם אין דעתנו כזו, מן הראוי להתייחס לכך.

---

[16] Dan Hunter "Cyberspace as Place and the Tragedy of the Digital Anticommons" 91 CALIF. L. REV. 439 (2003).

[17] זהו אתר כבן שלושים שנה המכיל את הטקסט המלא של אלפי יצירות ובאמצעות מתנדבים מעלה לרשת עוד ועוד יצירות ספרותיות. כתובתו היא: http://www.gutenberg.net/index.shtml (בוקר לאחרונה בפברואר 2003).

[18] ישנן כמובן מספר אתרים המציגים מפות עתיקות של ירושלים, ראו למשל: http://maps-of-jerusalem.huji.ac.il/.

בתי המשפט

68. בכל מקרה, גם אם התפיסה של האתר כמקום בעייתית היא, היא נוחה לשימוש והתובע השתמש בה רבות. התובע דימה שוב ושוב את מעשי הנאשם לאדם הזורק אבן (או נוצה) על קיר ברזל או קיר נחושת (עמ' 20 לסיכומיו). במקום אחר השווה אותו לאדם הנוקש על הדלת, מנסה לפותחה, בודק מנעולים, כו' (עמ' 21 לסיכומיו ובעוד מקומות).

69. מהסיבות שהזכרתי, היקש זה איננו במקומו. אם כבר נשתמש במטפורה, דוגמא טובה יותר תהיה לנהג הנוסע בכביש השייך לכולם ותוך כדי נסיעה רואה מכוניות אחרות שיש בהן בעיות ותקלות. בעיות כגון נקר בצמיג, עשן יוצא ממכסה המנוע, דלת פתוחה וכהנה וכהנה. דרך אחרת היא להשוות בדיקת האבטחה לאדם המבקר במוזיאון ברשות ותוך כדי הביקור מציץ ומסתכל על פתחי החירום, חלונות המוזיאון ועוד. גם אם יראה הדבר כלא נימוסי, בוודאי שאין מדובר פה במעשה פלילי.

<u>בדיקת אבטחתו של אתר איננה אסורה לכשעצמה ותלוייה בנסיבות</u>

70. לאור כל מה שכתבנו למעלה, מה צריכה להיות העמדה המשפטית לגבי בדיקת אבטחתו של אתר? האם מותר לאדם לבדוק את אבטחתו של אתר אחר שאיננו שייך לו?

71. מסקנתנו בעניין זה פשוטה וחד משמעית. אין אפשרות לקבוע באופן מוחלט כי בדיקת אבטחת אתר היא תמיד אסורה או תמיד מותרת. הסיווג המשפטי כמותר או אסור תלוי בנסיבות הספציפיות שבהן נעשתה הבדיקה, במטרה שבשלהן נעשתה, ובכוונתו של הבודק. אין כל אפשרות לנתקה מהן. ונדגיש, הכוונה היא לבדיקת אבטחה <u>ולא</u> לחיפוש חורי אבטחה כשלב מקדים לחדירה לא חוקית.

72. ישנה תועלת חברתית בכך שאתרי אינטרנט ייבדקו על ידי הגולשים ויוזהרו על ידם אם מצאו הללו פרצות כלשהן. יתירה מזו, הייתי מעז לומר שאין כל פסול שגולשים יפרסמו ברבים אתרי אינטרנט (ובעיקר שרתי אינטרנט) שאינם מאובטחים. אם רשימה כזו תפורסם ברבים, יהווה הדבר תמריץ וזרז לאחראים לתקן את חורי האבטחה שלהם. גולשים הבודקים את פגיעותם של אתרים פועלים במידה מסוימת לטובת הציבור ואם עושים זאת הם בכוונה טובה וללא להזיק אף ברוכים יהיו.

בתי המשפט

73. כדי להעמיד דברים על דיוקם, צריך להזכיר שבדיקת אתר בתוכנות אבטחה היא פעולה קלה מאד לביצוע. כל שצריך הבודק לעשות הוא להכניס את כתובת האתר לתוכנה והיא כבר מבצעת את השאר. למען הסר ספק, הרי מדובר בפעולה שנעשית מאות ואלפי פעמים כל יום על אתרים שונים ומשונים. כפי שציין מומחה האבטחה מר אופיר ארקין, יש לו אלפי התראות מסוג זה כל יום (פרו' מיום 18.12.03 עמ' 30 ש' 5-3). גם עד התביעה אריק וולף העיד כי יש להם כל יום מאות התקפות כאלה (פרו' עמ' 9 ש' 26). העד גם הודה בהגינותו כי מדובר בעשרות אלפי או מאות אלפי "התקפות" מעין אלו. דהיינו, מדובר בתופעה יומיומית וכללית.

74. למען הסר ספק, נדגיש שוב שהפעולה המותרת היא בדיקת אבטחת אתר ותו לא. כל פעולת בדיקה שמלווה בחדירה לא חוקית, מלמדת כי עצם הבדיקה מהווה חלק מהחדירה ובוודאי תהווה ניסיון.

<u>מדוע בעל אתר איננו יכול "לוותר" על בדיקת הגולשים האחרים?</u>

75. בעל אתר אינו יכול לוותר "ולגרש" גולשים המסתכלים על אתרו. מבחינת מדיניות ציבורית לא יהיה זה נבון להתיר לבעל אתר להכריז בקול גדול כי אין הוא מעוניין שמאן דהוא יבדוק את אבטחתו. בוודאי ובוודאי אין לאפשר לו לבקש כי מי שעושה כן ייחשב כעבריין פלילי. זאת משום שכל האתרים באינטרנט מקושרים אחד לשני ופגיעותו של אחד פוגעת גם באחר.

76. כפי שהראינו מקודם, אחת ההתקפות הידועות ביותר מכונה DOS (Denial of Services) ובנויה על "הפגזת" שרתים בבקשות שירות מזוייפות עד שהללו קורסים. אולם לצורך כך צריכים המתקיפים להשתלט על שרתים שאינם שייכים להם כדי שהללו גם כן ישלחו בקשות שירות באופן מופרז. דהיינו, התוקף מחפש ברשת מחשבים פגיעים כך שיוכל להשתלט עליהם חלקית ולגרום להם לבקש שירות מהשרת המותקף.

77. כל מחשב פגיע ברשת מהווה איום לא רק לבעליו ולתוכנו, אלא גם למחשבים אחרים המוגנים היטב. זאת משום שניתן להיעזר בו על מנת לתקוף אתרים ושרתים מוגנים. במילים אחרות, שרת שאיננו מאובטח כיאות מהווה סיכון לשרתים אחרים מאובטחים. העובדה שבעל

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

השרת הלא מאובטח איננו מעוניין כי יבדקו את אבטחתו, איננה משנה כהוא זה מסיכונו לשרתים מאובטחים.

78. נסתכל לדוגמא על וירוס מחשבים המתפשט ברשת במהירות הבזק. הוירוס מגיע לרשת/מחשב לא מוגנים, משכפל עצמו, ושולח עצמו דרך אותו מחשב לכל הנמענים הרגילים של המחשב. אם המחשב איננו מאובטח, הוא גורם נזק לא רק לעצמו אלא לכל אלו המתקשרים אתו בדרך כלל. יתירה מזו, גם אם המחשב מאובטח, הרי נגרם לו נזק בכך שהתעבורה ממנו ואליו נסתמת עקב עודף תעבורה. בצורה דומה למדי ניתן להסתכל על מה שמכונה "דואר הזבל" (spam mail). לו כל השרתים והמחשבים היו מוגנים כנגד דואר זבל, ואוסרים על שולחי דואר זבל לעבוד עימם, הייתה התופעה נמנעת או לכל הפחות פוחתת בהרבה.

79. נסתכל על דוגמא אחרת של זיוף מספר IP. ישנם גולשים שאינם רוצים כי מספרם ייודע (בדרך כלל, לא מסיבות מהוגנות). התוקף שולח ליעד התקיפה מנה כאשר כתובת המקור הכתובה בחבילה איננה הכתובת האמיתית. ליעד אין כל אפשרות לדעת את מקור המנות משום שהללו עברו דרך מחשבים רבים בדרך. לצורך כך ישנו מנגנון הגנה שמפעילים הנתבים ברשת הבודקים האם הכתובת על המנה המגיע אליהם היא אכן כתובת המחשב ממנו נשלחה. הגנה זו יעילה בעיקר עם יציאת המנה ממחשב התוקף, שכן רק הנתב הראשון יודע מיהו המחשב האמיתי. אולם אם הנתב הראשון איננו מפעיל את מנגנון ההגנה, יוכל התוקף לזייף מספרים באופן חופשי.

80. דוגמאות אלו מראות כי כל המשתמשים באינטרנט תלויים זה בזה וערבים זה לזה. כמאמר חז"ל בנושא שונה במקצת. **"אמר רבי שמעון בר יוחאי: משל לבני אדם שהיו יושבין בספינה נטל אחד מהן מקדח והתחיל קודח תחתיו. אמרו לו חבריו מה אתה יושב ועושה? אמר להם מה אכפת לכם? לא תחתי אני קודח? אמרו לו שהמים עולין ומציפין עלינו את הספינה".**[19]

81. כל מי שבקיא בתחום יודע ומבין כי ספינת האינטרנט תלוייה בכל גולשיה והמחוברים אליה. רשת האינטרנט נוסדה, התפתחה וקיימת כיום בזכות כל אותם פרטים התומכים,עוזרים, ודואגים לשלמותה. מדיניות ציבורית נכונה ונאותה חייבת להתבסס על כך ולעזור במגמה זו.

[19] ויקרא רבה (וילנא) פרשה ד ד"ה ו תני חזקיה

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

כיצד נדע איזו בדיקת אבטחה תחשב כאסורה ואיזה כמותרת ואולי אף רצוייה?

82. כפי שהסברנו מקודם, עצם הבדיקה איננה חדירה. אולם ברוב הפריצות האסורות, מהווה הבדיקה שלב מקדים. כדי שניתן יהיה לפרוץ, צריך לוודא כי חור אבטחה קיים. נכון הוא כי אם מדובר בניסיון פריצה ספציפי (כמו וירוס מחשב מוגדר), הרי התוכנה בודקת את פגיעותו של המחשב המותקף בנקודה מסוימת בלבד. אולם פעמים רבות נעשה ניסיון כללי למצוא את כל נקודות החולשה של מחשב כלשהו.

83. אם הבדיקה מהווה שלב מקדים לניצול חורי אבטחה ולחדירה למחשבים שונים, הרי בדיקה זו מהווה ניסיון לעבירה. אם אבל מהווה הבדיקה מעשה עצמאי לחלוטין שאין מטרתו פגיעה, הרי היא כשרה ולעיתים למהדרין. נסתכל על מקרה שבו אדם רוצה לבצע עסקה כלשהי עם אתר אינטרנט (מכירה וקנייה למשל) וברצונו לבדוק האם אתר זה מאובטח כדבעי אם לאוו. מה רע בכך שיכול להריץ תוכנת בדיקה על אותו אתר?

84. אם לעומת זאת אנו מוצאים במחשב הבודק תוכנות תקיפה שאינן רק בודקות אלא גם מזיקות; אם אנו רואים סימנים כי לאחר הבדיקה נעשו פעולות אחרות; אם הבדיקה היוותה שלב; אזי עצם הבדיקה מהווה ניסיון אסור. כפי שהסברנו קודם לכן, יש הבדל מהותי בין בדיקת חורי אבטחה לבין ניצולם כך שבפועל קשה לטעות בכך.

85. יושם לב שלא התייחסתי ליסוד הנפשי הדרוש אם כי לדעתי מדובר על יסוד נפשי זהה לכל עבירה פלילית. דהיינו, הוראות סעיפים 20-19 לחוק העונשין יחולו גם כאן.

על הצורך לפרש את חוק המחשבים בצורה התואמת לרוח ומבנה האינטרנט

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

86. ישנם ויכוחים עקובים מדיו על מטרות החקיקה. יש שסוברים שעל החוק לשקף את ערכי החברה, הגישה הכלכלית טוענת שמטרתם היא למקסם את התועלת הציבורית, והמרקסיסטים סבורים שהחקיקה באה לעזור למעמד השליט להנציח את כוחו. ועוד לא נגענו אפילו בקצה קצהו של מיגוון הדיעות העוסקות בכך. המשותף אבל לאלו ולאלו הוא הסכמתם כי לא ניתן להפריד את החוק מהמציאות עליה הוא חל.

87. עמדתנו העקרונית היא כי יש להיזהר בהיקשים מחוקים פליליים רגילים לחוקים הנוגעים לעולם האינטרנט. החוקים הפליליים הרגילים מתייחסים לעולם המבוסס על קניין פרטי ברור ומוגדר, היראַרכיה נוקשה, אינטרסים פרטיים, ושחקנים הדואגים בראש ובראשונה לעצמם. האינטרנט מבוסס על שיתופיות, התנדבות, אימון, הסכמיות, ומשאבים העומדים לשירות הכלל.[20]

88. למטבע כמובן יש שני צדדים. אותו אימון ממש בקהילת האינטרנט שהביא לפריחתו ולשגשוגו, הביא עמו גם תופעות שליליות. הפתיחות והשיתוף יכולים להיות מנוצלים לרעה והם אכן מנוצלים כך לעיתים. תופעת "דואר הזבל" (spam) היא דוגמא בוטה לשימוש באימון שניתן במשתמשים. בגלל הארכיטקטורה של האינטרנט והשוויון בחלוקת המשאבים, הגענו למצב שבו אחוז גבוה מכלל הדואר האלקטרוני ברשת מורכב מהודעות "זבל" שאיש לא ביקש לקבלם והן מגיעות לציבור בעל כורחו.

89. כשמדובר על חקיקת אינטרנט, יש לפרשה בצורה שתעזור לעולם האינטרנט להמשיך להתפתח קדימה ולטובת הציבור, ולא בצורה שתגביל, תפריע, ותעכב התקדמות זאת.

90. על פי עיקרון זה, בדיקת אבטחת אתרים היא פעילות חיובית בעיקרה שעקרונית צריך לעודדה ולהיזהר מלפגוע בה. אפילו אם נראה כי יש בכך מעין "חוצפה" מסוימת כלפי בעלי האתרים. אולם חובה להדגיש אין מדובר פה בסלחנות לשמה. אותו עיקרון ממש ידרוש פרשנות מחמירה, תקיפה, ואפילו קשה כנגד אלו אשר פוגעים בהתנהגותם בתשתית האינטרנט, תשתית שכפי שהזכרנו היא פגיעה מאוד בגלל השיתופיות ואמון המובנות באינטרנט. מפיצי וירוסים

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

ותכנים מזיקים אחרים ראוי להם כי ייענשו קשות, ופרשנות נכונה תהיה זו שתרחיב את אחריותם ולא תיתן להם להתחמק בנימוק זה או אחר.

ומהתאוריה למעשה - מה עשה הנאשם שלפנינו?

91. חובה להזכיר ראשית את כתב האישום בו הואשם הנאשם ונצטטו על כל חלקיו.

"1. ביום 22.9.2002 סמוך לשעה 19:25 חדר הנאשם לחומר מחשב הנמצא במחשב שלא כדין, מביתו בירושלים.

2. הנאשם התחבר באמצעות התקשרות לאתר האינטרנט של "המוסד לתפקידים מיוחדים" (המוסד) של מדינת ישראל, בכתובת www.mohr.gov.il **(להלן: "האתר").**

3. הנאשם הפעיל כנגד האתר תוכנת פיצוח ופריצה, המשגרת עשרות רבות של ניסיונות פיצוח שונים של קודי ההגנה השונים והרבים של האתר.

4. הנאשם אף הפיק מהתוכנה פלט של נתונים תוצאות "ההתקפה" על האתר, פלט אשר מאפשר לדעת מהם כשלי אבטחה באתר.

5. הנאשם ביקש ברשת האינטרנט סיוע בקריאת פלט הנתונים שאותו לא ידע לקרוא בעצמו. הנאשם ביצע האמור למרות ששיער כי הדבר איננו חוקי"

92. נדמה לי שטענת התביעה בדבר תוכנת פיצוח ופריצה המשגרת עשרות רבות של ניסיונות פיצוח נגד קודי ההגנה השונים והרבים, הייתה מוגזמת במעט ולא אוסיף בכך.

93. לאור העדויות בתיק אני קובע את העובדות הבאות.

- הנאשם איננו מבין באבטחת מחשבים ואיננו מתיימר להבין.

---

[20] על השלכות רשת האינטרנט על המשפט המהותי ראו א. טננבוים "השלכות רשת האינטרנט על המשפט המהותי" שערי משפט א(2) כסליו תשנ"ח עמ' 133- 188. המאמר מופיע ברשת במספר מקומות ראו הכתובת:http://www.mishpat.ac.il/courses/tennenbaum/index/main/articles/data/Internet%20Implicitions-Heb.pdf

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

- הנאשם התעניין זמן ממושך בהצטרפות למוסד. כשעלה אתר המוסד לאוויר, נכנס הנאשם לאתר המוסד מתוך מטרה להצטרף לשירותיו, וחשד כי מדובר באתר לא מאובטח. אין באתר כל דרך להתקשרות עם מנהליו מלבד טופס בקשת הצטרפות, כך שלא ניתן לברר זאת עם האחראים לו.

- הנאשם שלפנינו, פנה לאתר העוסק בין היתר באבטחת מחשבים (וגם בפריצתם) והוריד ממנו תוכנה חינמית לבדיקת כשלי אבטחה. את התוכנה הסצפציפית בחר היות ולפי האתר, הייתה תכנה זו פופולרית ומספר ההורדות שלה היה הגבוה ביותר. מדובר בתוכנה אנונימית שהנאשם לא הבין בה רבות. כמו כל התוכנות מסוג זה, כל שצריך בעיקר הוא להכניס את כתובת האתר וללחוץ start והתוכנה עושה את היתר.

- התוכנה הפיקה לוג (פלט) מסויים שאותו לא הצליח הנאשם להבין. הוא פנה לבקשת עזרה במספר ערוצים צ'טים באינטרנט אך לא נענה.

- משהתייאש הנאשם עזב את כל הענין ואף מחק את התוכנה.

94. יושם לב כי ישנן מספר נקודות שהצדדים התנצחו בהם קשות בטיעוניהם לפני אך לא מצאתי כל סיבה מהותית להתייחס אליהן. כך למשל, הייתה מחלוקת קשה אם היה אתר המוסד מאובטח ביום זה או אחר שקדם למעשה הנאשם (אם כי אין מחלוקת שהאתר היה מאובטח ביום בו נכנס אליו הנאשם). התביעה למשל טענה כי האתר היה מאובטח והנאשם ידע זאת בבירור. ההגנה טענה לעומת זאת כי האתר לא היה מאובטח. דעתי היא כי האתר היה בוודאי מאובטח אולם לא ברור עד כמה הנאשם יכל לדעת זאת ובכל מקרה אין הדבר משנה.

95. הצדדים התנצחו גם קשות בשאלה האם נרשם הנאשם לאתר המוסד מתוך מטרה להתקבל אליו אם לאוו. לטענת התביעה, העובדה שלא נרשם מראה שלא ענייני אבטחה היו בראש מעייניו. ההגנה טוענת שהנאשם נרשם גם נרשם. דווקא בשל כוונתו להירשם ולחשוף פרטים אישיים ביקש לדעת כי האתר אליו הוא שולח את פרטיו איננו פרוץ. נקודה זו איננה עקרונית לטעמי.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

96. מסקנתי היא כי הנאשם אכן סבר שהאתר איננו מאובטח וזו הסיבה שניסה לבודקו. לטענת התביעה, הנאשם ביקש לבודקו כדי להרשים יותר מאוחר את אנשי המוסד או כל גוף אחר כטענת התביעה. לטענת ההגנה עשה זאת כדי להיות בטוח שנתונים אותם ביקש לשלוח יהיו מאובטחים. סביר להניח ששני הצדדים צודקים במידה זו או אחרת, אך לא מצאתי כי נקודות אלה רלוונטיות לאור המסקנה שהגעתי אליה ותפורט מאוחר יותר.

<u>דוגמאות לבדיקות שערכה התוכנה בה השתמש הנאשם</u>

97. לא ניכנס לכל הכשלים שבדקה אותה תוכנת בדיקה, אולם נציג לדוגמא שלושה מהם. בעמ' 1 של ת/ 4 ניתן לראות כיצד נרשמו 3 נסיונות לפורט 0. כפי שהזכרנו שליחת מנה לפורט 0 יכולה ליצור בעיות ורוב התוכנות לבדיקת אבטחה מבצעות זאת.

98. דוג' אחרת היא בשורה האחרונה של עמ' 1 שבה מופיעה הפקודה cmd.exe. מדובר בפקודה הבודקת האם ניתן להיכנס מחוץ למערכת ההפעלה dos. הפקודה cmd היא פקודה חוקית ולגיטימית בכל מערכת חלונות המעבירה את המשתמש ישירות לרמת dos (מערכת ההפעלה שקדמה לגרסאות החלונות אך משובצת בה). מי שנכנס ל- dos יכול לבצע מספר פעולות לא סימפטיות. החידוש בכך הוא, שפקודה זו בודקת האם ניתן יהיה להיכנס למערכת dos מחוץ לאתר. שוב, כמו בכל כשל אבטחה אין בכך מספיק. גם אם יודעים אנו שניתן להיכנס מבחוץ למערכת הפעלה dos צריך להיות מומחה ולהבין היטב אם ניתן לגרום נזק ואיזה נזק ניתן לגרום.

99. דוג' אחרת היא בשורה 17 מלמטה המשתמשת web-misc webhits.exe. בשורה זו נבדק האם ניתן להפעיל את הפקודה webhits מחוץ לאתר. זוהי פקודה הקשורה לאפליקציות web ואם אכן ניתן להפעילה מבחוץ ואם אכן המפעיל הוא מומחה, אז יכול המפעיל לגרום לכך שאפליקציות מסויימות יהיו חשופות לו. תיאורטית, אם מדובר באינפורמציה כגון מספרי כרטיסי אשראי באפליקציה שעוסקת בקניות, יכול המומחה להשתמש בכך ולנסות לברר את מספרי כרטיסי האשראי. ויושם לב, הבדיקה הזו איננה אלא שלב ראשוני שאחריו יש צורך בידע רב כדי להמשיך הלאה. יושם לב לנקודה נוספת והיא, שאם עוסקים אנו באתר שאין בו טרנזקציות או אפליקציות ב- web, לא יטרח אפילו בעל האתר לעיתים לחסום "חור" זה, מפני שהדבר איננו נוגע לו כלל.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

100. התרשמותי היא כי אין מדובר בתוכנה כה יעילה כפי שביקש מאיתנו ב"כ המאשימה להחליט. אולם מדובר בתוכנה המאפשרת בדיקת כשלי אבטחה רבים שהייתה טובה לזמנה. סביר להניח שזוהי הסיבה שכמות ההורדות שלה מהרשת על ידי גולשים שביקשו להשתמש בה הייתה הגדולה ביותר.

<u>כיצד הגיעה המשטרה לנאשם?</u>

101. למען הסיר ספק הרי אתר המוסד איננו נמצא על מחשבי המוסד ואין לו שום קשר למחשבי המוסד (ורצוי שכך). מדובר באתר היושב על מחשב הנמצא באתר השרתים של משרדי הממשלה (תהילה). תהילה היא גוף המתחזק אתרים רבים של משרדי ממשלה שונים ובתור שכזה יש לו כמובן אמצעי אבטחה משלו. בין אמצעי אבטחה אלו, ישנה תוכנת חומת אש[21] וכן תוכנת snort. תוכנת ה- snort גילתה מאפיינים של בדיקת כשלי אבטחה כפי שניתן לראות בתדפיס שהוגש לי בענין ת/ 4.

102. מאפיינים אלו שגילתה התוכנה נשלחו על ידי "כתובת" בעלת מספר ה - IP 62.0.144.27 (כפי שניתן לראות בתדפיסי ת/4 ו - ת/5). זוהי כתובת ישראלית שהסתבר שהיא שייכת לספק האינטרנט netvision (להלן: "הספק"). הספק נותן את הכתובת באופן אקראי ללקוחותיו המתחברים דרכו (כל פעם ללקוח אחר, אך כמובן אין אפשרות שלשני לקוחות יהיה אותו מספר באותו זמן).

103. יש בידי הספק רישום קבוע של הלקוחות שקבלו את מספרי ה - IP בכל עת ושעה כולל מספר זה. המשטרה פנתה לספק ובצו בית משפט ביקשה לדעת מי השתמש במספר הנ"ל ביום העבירה (שם משתמש, ומספר הטלפון ממנו השתמש). חברת netvision מסרה את פרטי המשתמש, חברת הטלפון (בזק) מסרה את פרטי הקו וכך הגיעו לנאשם שכלל לא ניסה להסתתר.

<u>המסקנה החד משמעית - הנאשם לא עבר עבירה כלשהי</u>

---

[21] כפי הנראה מהתדפיס מדובר על fire wall של מכונת linox.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

104. מכל הנסיבות האופפות את האירוע ברור כי הנאשם לא עבר עבירה כלשהי. הנאשם לא ניסה להסתיר דבר והחל מהרגע הראשון שיתף פעולה עם חוקריו באופן מלא. הנאשם צווח ככרוכיא החל מהרגע הראשון שכל שביקש לעשות היה לבדוק אם אתר המוסד מאובטח אם לאוו. לא נתפס אצלו כל חומר חשוד ו/או כל תוכנה שיכלה להשתמש בחורי אבטחה ולנצלם. כל מה שידוע לתביעה על התוכנה בה השתמש ועל פעולותיו למדנו מפיו ומפיו בלבד שכן עד היום לא ברור באיזה תוכנה השתמש. אוסיף גם כי הנאשם רחוק מלהיות מומחה אבטחה/פריצה ואף לא התיימר להיות כזה. גם העובדה שכל פעולותיו נעשו בריש גלי ללא כל ניסיון להסתיר את כתובתו (האינטרנטית) מלמדת על חוסר אשמתו הפלילית.

105. יש להדגיש כי אילו היה הנאשם נתפס בשקר כלשהו, או היה מסתיר פרטים מחוקריו, או הייתה מתגלית אצלו תוכנת פריצה מזיקה, היה הדבר יכול להיחשב כנסיבה לרעתו ולהוכחה כי מדובר בניסיון לחדירה. אולם דבר מאלו לא נמצא.

106. התרשמתי מהנאשם ושמעתי את עדיו ואני קובע עובדתית וחד משמעית כי הנאשם לא פרץ ולא ביקש לפרוץ אלא ניסה לבדוק את אבטחת האתר. שוב, אין אני קובע מסמרות אם עשה זאת משום שביקש להרשים את מנהלי האתר (כגרסת התביעה) או משום שרצה להיות בטוח שהוא שולח את פרטיו לאתר בטוח (כגרסתו). סביר להניח שהאמת אי שם באמצע אולם אין זה רלוונטי לענייננו.

107. הסניגוריה התעמקה רבות בשאלת היסוד הנפשי הנדרש לביצוע העבירה. אולם לאור קביעותי העובדתיות כי לא הייתה לו כל כוונה, אין צורך להתפלפל בשאלה זו.

אשר על כן מן הראוי לזכותו מכל אשמה.

<u>האם זכאי היה הנאשם להגנה מן הצדק?</u>

108. הצדדים שפכו דיו כמים בשאלה זו של הגנה מן הצדק ולו מחמת כבודם מן הראוי להתייחס אליה. הדברים לא נאמרו בפירוש אולם ברור לשני הצדדים כי אם לא היה זה אתר המוסד, אלא למשל אתר האגף לדייג ולחקלאות מים במשרד החקלאות, או אתר העוסק בפרשת

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

השבוע במחלקה למשפט עברי במשרד המשפטים,[22] איש לא היה טורח אפילו להעיף מבט לכיוון הנאשם. קל וחומר לא להתאמץ עד כדי לחפשו, למוצאו, לחוקרו, ולהעמידו לדין.

109. תמצית ההגנה בנקודה זו פשוטה ובהירה. מאות "התקפות" מעין אלו נעשות על אתרי הממשלה מדי יום ביומו, מה נטפלה לה התביעה מכולם דווקא לאבי מזרחי הנאשם? (האמת היא שההגנה לא דייקה, מדובר על אלפי התקפות אם לא עשרות אלפי התקפות). אלא מאי? (וזאת אומרת ההגנה ברמז דק כפילון) רצה מאן דהוא להפגין שרירים ולהראות כי עם ישראל חי וכל המתעסק עם המוסד מרה תהיה אחריתו, ונפל הפור על הנאשם דווקא, ולשומע ינעם.

110. תמצית דברי התביעה גם היא פשוטה. לא ניתן תמיד לאכוף את החוק נגד כולם והמשטרה עשתה ועושה כמיטב יכולתה. רוב ההתקפות נעשות מכתובות מחוץ לישראל שקשה לאתרם, ובכלל מדובר בהתקפה קשה יחסית. ובאשר לענייננו מדובר באתר עם השלכות ביטחוניות מי ישורם, ואין כלל להתפלא על כך שדווקא באתר זה הוחלט למצות את הדין עד תומו.

111. הגנה מן הצדק היא ברייה מוזרה בעולם המשפט. לשם הגנה זו אין נפקא מינא כלל אם אכן ביצע הנאשם את העבירה אם לאוו. יתירה מזו, הגנה זו איננה מופיעה אפילו ברמז בחקיקה וכל כולה היא יציר הפסיקה.

112. מקובל שישנם שלושה מודלים עיקריים בסוגיית ההגנה מן הצדק. המודל הראשון הוא מודל "הסמכות הטבועה". על פי מודל זה בסמכותו הטבועה של בית המשפט לבדוק האם לא נעשה שימוש לא ראוי בהליך הפלילי למטרות לא לו. בית המשפט הוא זה האחראי ששום איש וגוף, כולל רשויות המדינה, לא ישתמש בהליך הפלילי למטרות לא ראויות.

113. המודל השני הוא מה שמכונה "המודל המנהלי". על פי מודל זה בית המשפט שם תחת ביקורתו את שיקוליה של הרשות המנהלית להעמיד נאשם כל שהוא לדין, ואת התנהלותה במהלך המשפט. בדרך כלל נבדקים שיקולים מנהלתיים על ידי בית המשפט הדן בעתירות כאלו, אך לא

---

[22] כתובותיהם הן בהתאמה: http://www.mop-zafon.org.il/fish/index.html ו -
http://www.justice.gov.il/MOJHeb/MishpatIvri/ParashotShavua/ ואין אנו מתכוונים לזלזל חס וחלילה בגופים אלו וחשיבותם.

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

כאן. ייחודה של ההגנה מן הצדק הוא שבמקרים מסוימים בהם "אי הצדק צועק לשמיים", אותה הערכאה שדנה בדין הפלילי היא זו שגם תבדוק את שיקול הדעת המנהלי להעמיד לדין.

114. המודל השלישי והאחרון הוא המודל החוקתי הקובע כי צריך במקרים קיצוניים לבדוק אם הייתה פגיעה כל שהיא בזכות להליך הוגן. במידה והייתה פגיעה כזו, יש לבדוק האם למרות שהופרה זכות זו מן הראוי להמשיך בהליך הפלילי. נכון הוא שבמשפט הישראלי אין לנו את הזכות להליך הוגן (due process), אולם כרגיל במשפטנו לאחרונה, גם פה נטען כי ניתן לגזור את הזכות להליך הוגן מחוק כבוד האדם וחירותו.[23]

115. נכון הוא שישנם מלומדים הרואים בהכרה בהגנה זו התקדמות.[24] דעתו של בית משפט זה שונה לחלוטין. ישנה מידה רבה של אי נוחות בשימוש בהגנה מן הצדק. אחרי ככלות הכל יש חוק בישראל ואמונים אנו על שלטון החוק. מי שהפר את החוק, ולכל הדעות עשה זאת, מניין החירות לבית משפט לקבוע אם ההליכים הפלילים נגדו ייפסקו? אפילו נהגה הרשות שלא כדין בקטע זה או אחר, מה עניין זה לעניין הפרת החוק של הנאשם? הניסיון מלמד שכאשר הצדק נפגע קיימות כבר לנפגע הגנות משפטיות שפותחו במהלך השנים. אין לכן צורך להוסיף עליהם הגנה חדשה שאיננה מוגדרת היטב. גם כך בוקרו בתי המשפט (ואולי בצדק) על שלקחו לעצמם סמכויות לא להם ואינני משוכנע שיש צורך להוסיף בכך.

116. המציאות גם מלמדת שטענת ההגנה מן הצדק מועלית דווקא על ידי אלו הרחוקים מלהיות חלשים ומדוכאים. טענת הגנה מן הצדק הועלתה לא פחות ולא יותר מאשר במשפט "הבנקאים" **(ע"פ 2910/94 יפת ואח' נ. מדינת ישראל פ"ד נ(2) עמ' 221).** תהיה דעתנו האישית אשר תהיה על משפט זה ועל תוצאותיו, אך אין חולק כי הנאשמים בו היו רחוקים מאוד מלהיות שייכים לחלק החלש של האוכלוסייה. האם דווקא מגזר זה של הנאשמים הוא זה שצריך הגנה ייחודית של הגנה מן הצדק?

---

[23] ראו בעניין שלושת המודלים את ספרו של ישגב נקדימון "הגנה מן הצדק" נבו הוצאה לאור תשס"ד – 2003.

[24] מקריאת ספרו של נקדימון נראה שהוא סבור כך. זוהי כנראה גם דעתם של סגל וזמיר במאמרם החדש יחסית (פרופ' זאב סגל ואבי זמיר "הגנות מן הצדק כיסוד לביטול אישום – על קו התפר בין המשפט הפלילי והמשפט הציבורי" הפרקליט מז' חוברת א' עמ' 76-42).

בתי המשפט

בית משפט השלום ירושלים | פ 003047/03

בפני: שופט: טננבוים אברהם.נ | תאריך: 29.2.2004

117. ישנן דעות מכובדות הטוענות כי רצוי לה להגנה זו שלא נולדה משנולדה. ואם אין מנוס וכבר נולדה, אזי גם אז מוצדק קיומה רק לשעת הדחק ולעת מצוקה. בית משפט זה שייך לאסכולה זו הסוברת כי הגנה מן הצדק רצוי שתיטען אך ורק במקרים קיצוניים ויוצאי דופן. מקרים שבהם חוסר הצדק בהליך בולט וזועק לשמיים. מקרים שבהם כל שומע תיצלנה שתי אוזניו ויש הסכמה גורפת כי אי-הצדק ברור. לא זהו המקרה שלפנינו. התביעה אומרת בפירוש ובלשון ברורה כי לו ניתן היה הייתה מעמידה לדין רבים אחרים אך מה לעשות והמשאבים מצומצמים ואין אפשרות לכך. אין רע בכך שמקרה אחד יעמוד לדין ולו רק ללמד את הציבור כי מעשה זה פסול ואסור. דעתי לכן נוטה לקבוע כי לא עומדת לנאשם הגנה מן הצדק במקרה זה אולם אין טעם לקבוע בכך מסמרות לאור מסקנתנו הקודמת.

סוף דבר

118. לסיכומו של דבר, לאחר ששמעתי את הצדדים ולאור מכלול הראיות והעדויות כפי שהסברנו, החלטתי לזכות את הנאשם מכל אשמה.

בהזדמנות זאת מן הראוי לשבח את התובע עו"ד עמוס כהן והסניגור עו"ד עמרי כבירי שניהלו את המשפט ביעילות ובהגינות ולא הערימו קשיים פרוצדוראליים זה על זה (ובתיק מעין זה, הערמת קשיים קלה להפליא).

זכות ערעור תוך ארבעים וחמישה יום לבית המשפט המחוזי.
המזכירות תשלח העתק פסק הדין לצדדים.
ניתן בלשכתי בהעדר הצדדים ובהסכמתם היום יום ראשון, ז' אדר תשס"ד (29.2.2004).

אברהם נ. טננבוים
שופט