

Open internet ports procedures

How to open access from outside the Technion/faculty?

We do not open access directly to local stations at the faculty for any service,

Please use faculty servers or lab servers for such access.

For lab servers please, ask your lab engineer to open a helpdesk case and to contact us with all the service port details.

הליך פתיחת גישה לשרת ברשת של הפקולטה

ההליך בא להסדיר את התנאים לפתיחת גישה מחוץ לטכניון ומחוץ לפקולטה לשרת הנמצא ברשת של הפקולטה. מטרת ההליך להסדיר את הטיפול השוטף בשרת ולמקד אחריות לתקינותו, המטרה גם לצמצם את הנזק שיגרם במידה ויקרה אירוע אבטחה באמצעות הגישה הזו. כדי להשלים את פתיחת הגישה יש למלא את כל התנאים הבאים:

1. על השרת להשתייך למערכת ניהול הרשאות חשבונות פקולטית ולא מנוהל עצמאית.
 2. לא קיים שרת אחר כבר קיים שמאפשר את אותה גישה.
 3. על השרת מותקן firewall מקומי וכל האמצעים המבטיחים אתה תקינותו. מסתמך נוהל התחברות לרשת הפקולטית.
 4. יש מדיניות פקולטית המופעלת על השרת.
 5. אחראי השרת חותם על הבקשה לפתיחת הגישה.
 6. אין גישה מהשרת לשטחי אחסון בפרוטוקולים לא מאובטחים.
 7. מופעל ניטור ודיווח לאחראי המערכת.
 8. מתבצע אימות של השרת ברשת. (בהתאם לתשתיות הקיימות)
 9. בכל מקרה של פריצה אחראי השרת עובד לפי נוהל אירוע אבטחה טכניוני תוך ידוע צוות המחשוב הפקולטי.
 10. פתיחת גישה לשרת תוקצב בזמן, בתום הזמן אחראי השרת יצטרך לבקש גישה מחדש.
 11. בנוסף אחראי השרת יזום סריקת מצב הפורטים הפתוחים ובדיקתם מחדש בכול תחילת סמסטר ופעם נוספת חודש לאחר מכן.
 12. כל שינוי במצב השרת או השרות כולל העברת אחריות על השרת תיעשה בתיאום מלא עם צוות המחשוב הפקולטי.
 13. המלצה להתקין certificate חתום פקולטי לגישות מוצפנות.
- לאחר תום וידוא כל התנאים תועבר הבקשה למנהל firewall.

כאן הפירוט לפי מערכות הפעלה נפוצות:

דרישות סף משרת לינוקס לפני פתיחת ports

מנגנון AUDIT עובד הלוגים מתעדכנים.

מופעל firewall מקומי שמשאר רק את הservice פתוח.

עדכוני אבטחה מתבצעים באופן אוטומטי.

גישת SSH או כל גישה אחרת רק למשתמשים ללא הרשאות מיוחדות בפרוטוקולים מאובטחים.

יש איפת החלפת סיסמאות למנהלי המערכת המלצה להשתמש בפקודה chage .

יש שימוש בבקרת כניסה לגישה לשרת המלצה להשתמש במנגנון ה access.conf .

מותקנת תוכנת ניטור או יש להצטרף לשרות הניטור הפקולטי הקיים כבר.

המלצה לגבי התקנת שרות הפתוח ב firewall הטכניוניוני כגון APACHE יש לבצע מתוך repository של ההפצה ולא מקוד מקור. כך עדכוני האבטחה יכללו את התוכנה החדשה.

המלצה להתקין certificate שחתום על ידי רשות מוסמכת ולא self signed

דרישות סף משרת windows לפני פתיחת PORTS

Anti-virus installation + daily update enable log of all account and priv change events enable firewall Microsoft updates enabled. Change local admin username + complex password.:If in domain, move to a servers OU. do not leave in "Computers". And same as Linux for certs, manager, monitoring, etc.