Cloud Computing

LECTURE 10

מחשוב ענן

Cloud Computing Concepts

The cloud has five defining characteristics:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

מושגי מחשוב ענן

לענן תכונות מאפיינים מגדירים:

שירות עצמי לפי דרישה.

גישה לרשת רחבה.

איגום משאבים.

גמישות מהירה.

שירות נמדד

Service Models

There are four basic models with which clouds provide services:

- Software as a Service (SaaS) – applications in the cloud
- Platform as a Service (PaaS) – languages and tools to support application development in the cloud
- Infrastructure as a Service (IaaS) – processing, storage, network components in the cloud

Cloud computing implies export of processor, storage, applications, or other sources. Sharing resources increase security risks.

בגני שירות

יקום ארכיטקטורה בגנים כמותים אינם הענני

מספקים שירותים:

- תוכנה כשירות (SaaS) - יישומים בענן
- פלטפורמה כשירות (PaaS) - שפות וכלים לתכנות ביישומים בענן.
- תשתית כשירות (IaaS) - עיבוד, אחסון ורכיבי רשת בענן.

מחשוב ענן מרמז על יבוא כל מעבד, אחסון יישומים או מקורות אחרים. שיתוף משאבים מגביל את סיכוני האבטחה.

קיום גירות

לענן פרטי יש תשתית המנוהלות באופן בלעדי על ידי הארגון ובבעלותו, אלא ייתכן שגורם ענן יתקבל לצד שלישי.
ענן קהילתי משותף לעסקי ארגונים ומעניק בדרך כלל לבעיה מעניינת.

Service Models

A private cloud has infrastructure that is operated exclusively by and for the organization that owns it, but cloud management may be contracted out to a third party.

A community cloud is shared by several organizations and is usually intended to accomplish a shared goal.

A public cloud, available to the general cloud, is owned by an organization that sells cloud services.

A hybrid cloud is composed of two or more types of clouds, connected by technology that enables data and applications to be moved around the infrastructure to balance loads among clouds.

ענן ההיברידי מורכב משני סוגים או יותר שלא מאוחדים, המתוארים על ידי טכנולוגיה המאפשרת להביא נתונים ואפליקציות סביב התשתית כדי לאזן בין עומסים בין עננים.

Moving to the Cloud

Moving to a cloud can be difficult and expensive, and it can be equally expensive to undo. While every cloud offering presents its own set of risks and benefits, a number of guidelines can help you understand whether your functions and data should be migrated to a cloud environment, as well as which cloud offerings will be most likely to meet your security needs.

עוברים לענן

מעבר לענן יכול להיות קשה וקר, ולכן יכול להיות יקר לא בחוכמה לבטל. בעזרת שלל הדרכות ענן מדריך מורכב מהיבטים ומרווחים משלה. מספר הנחיות יכולות לעזור לך להבין אם יש להעביר את הפונקציות והנתונים שלך להעביר ענן, ושונים אילו הדרכות ענן המשמעות לסבוק את דרכי הטובות שלך.

Risk Analysis

Risk analysis should be a part of any major security decision, including a move to cloud services.

1. Identify access.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected loss.
5. Survey and select new controls.
6. Project savings.

ניתוח סיכונים

ניתוח סיכונים דרוש להיות חלק מכל בחלטה אבטחה משמעותית, כולל מעבר לשירותי ענן.

- זהה גישה.
- קבע נקודות תורפה.
- העלק את הסבירות לניצול.
- חשוב בהפסד הצפוי.
- הקר ובחר בקרים חדשים.
- חישוב בפרוייקט.

הערכת ספק ענן

הערכת ספקי ענן היא תהליך דו-שלבי:

1. קביעת דרישות הענן שלך

בעוד שרבים מהקריטריונים הבאים יהיו ספציפיים למערכת, הנה כמה קטגוריות המופיעות בדרך כלל:

- אפשרויות אימות והרשאות גישה
- יכולות הצפנה
- יכולות רישום
- תגובה לאירוע
- אמינות / זמן פעולה

2. קביעת הספקים שעומדים ברשימת הדרישות שנקבעה בשלב הראשון.

Cloud Provider Assessment

Assessing cloud providers is a two-step task:

1. Determining your cloud service needs.

   While many of the security controls will be specific to the system, here are a few categories that commonly appear:
   - Authentication, authorization, and access control options
   - Encryption capabilities
   - Logging capabilities
   - Incident response
   - Reliability/uptime.
2. Determining which providers meet the list of requirements you created in the first step.

החלפת ספקי ענן

נעילת ספק מתבטאת את ספקי בהחלפה שלך. רשאה מבלי עקב שמתמש אל, המעבר בין ספקי שירותים יכולה להיות יקרה. לרוב המצלבים יכול להבוך לחוביות אבטחה תשובה מכיוון שמשתמשים בטוחים לא רבים הקשורים לאבטחה ואמינות עשויה לגרום לשינוי בספקים:

1. לספק שלך יש בעיות אבטחה משמעותיות שלא ניתנות לתיקון קל.
2. הספק שלך משנה את הדרישות שלו או את מבנה ה-API כך שבוטל כבר לא תואם לדרישות שלך.
3. הספק שלך מעביר את פעילותו למדינה זרה שבה אסור לך לשמור את המידע שלך.
4. הספק שלך יוצא מהעסק.

Switching Cloud Providers

Vendor lock-in inhibits your switching providers.

When you are running a business that relies on cloud services, migrating between service providers can be expensive. Unfortunately, this can become an important security issue because many potential security- and reliability-related events might drive a change in providers:

1. Your provider is shown to have a major security vulnerability that cannot be easily repaired.
2. Your provider changes its features or API specification so as to no longer be compatible with your requirements.
3. Your provider moves its operations to a foreign country where you are prohibited from maintaining your data.
4. Your provider goes out of business.

מחסום ענן מגביר את הסיכון לנקודות כשל בודדות.

- גיבוי גיאוגרפי.
- גיבוי הפלטפורמה.
- מגוון תשתית.
- סינון דוא"ל.
- הגנת DDoS.
- ניטור רשת.

Cloud as a Security Control

Cloud computing mitigates the risk of single points of failure.

- Geographic diversity
- Platform diversity
- Infrastructure diversity
- Email filtering
- DDoS protection
- Network monitoring

Cloud Security Tools and Techniques

Using a public cloud service will likely mean sending private data to the service provider via the Internet and storing private data on the cloud provider's servers. While different cloud service models accord you different degrees of control over security, it is your own responsibility to choose cloud offerings that ensure, or allow you to ensure, that your data – as well as those of your partners and customers – are adequately protected from modification and disclosure.

כלים וטכניקות אבטחת ענן

השימוש בשירות ענן צי'רני פירושו כלל הנכונות שליחת נתונים פרטיים לספק השירות דרך האינטרנט ואחסון נתונים פרטיים על שרתי ספק הענן. בעוד שמודלים שונים של שירותי ענן מעניקים דרגות שונות של שליטה על אבטחה, באחריותך לבחור הצעת ענן שמבטיחה או משלבת לך להבטיח כי הנתונים שלך - כמו גם של השותפים והלקוחות שלך, מוגנים כראוי מפני שינוי ותשמיש.

Cloud Storage

When considering a cloud solution from a data storage perspective, you should think about a number of security-related issues:

- How sensitive is the data I'll be storing?
- Will I need to share the data with anyone and, if so, what kinds of access controls will I require?
- Are the data subject to export controls or other regulations?

אחסון בענן

כשאתה שוקל פתרון ענן מנקודת מבט לאחסון נתונים, עליך לתשוב על מספר סוגיות הקשורות לאבטחה:

- כמה רגישים הנתונים שאחסן?
- האם אצטרך לשתף את הנתונים עם שותפים, ואם כן, אלו סוגי בקרות גישה אצטרך?
- האם הנתונים נתונים לבקרת יצוא או לתקנות אחרות?

Cloud Storage

Shared storage involves a threat of access from sharing neighbors.

Changing cryptographic keys for large amounts of encrypted data is time consuming. A protocol using master and user keys makes changing efficient in use of time.

Sharing cryptographic keys with cloud storage providers potentially exposes sensitive data.

אחסון בענן

אחסון משותף כרוך בסיכון שלא גישה מצד שיתוף שכנים.

שינוי מפתחות קריפטוגרפיים לכמויות גדולות של נתונים מוצפנים לוקח זמן. פרוטוקול המשתמש במפתחות אב ומשתמש היופך את היעילות לשינוי בשימוש בזמן.

שיתוף מפתחות קריפטוגרפיים עם ספקי אחסון בענן עלול לחשוף נתונים רגישים.

Data Loss Prevention

Data Loss Prevention (DLP) can be difficult to accomplish with cloud storage.

One way to maintain DLP capability when moving to a public cloud is to force users to go through the company network to get there.

Another solution for maintaining DLP capability after moving to the cloud is to insert the DLP capability at the network boundaries of the cloud environment.

מניעת אובדן נתונים.

מניעת אובדן נתונים (DLP) יכולה להיות קשה להפעלה באמצעות אחסון ענן.
אחת הדרכים לשמור על יכולת DLP בעת מעבר לענן ציבורי היא לגרום משתמשים לעבור דרך החברה להגיע לשם.
ביתרון נוסף לשמירה על יכולת DLP לאחר מעבר לענן הוא הכנסת יכולת DLP בנקודות הכי קרובות לענן.

Cloud Application Security

The biggest adjustment you need to make when writing applications for cloud deployment is to understand how your threats change.

There are a couple of general threats that come up as a result of the cloud computing paradigm:

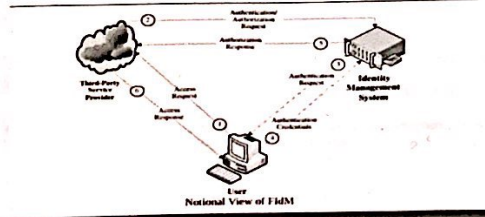
- Attacks against shared resources.
- Insecure APIs.

Unfortunately, short of extensive security testing of your cloud providers and partners, there is not much you can do to protect yourself from these issues.

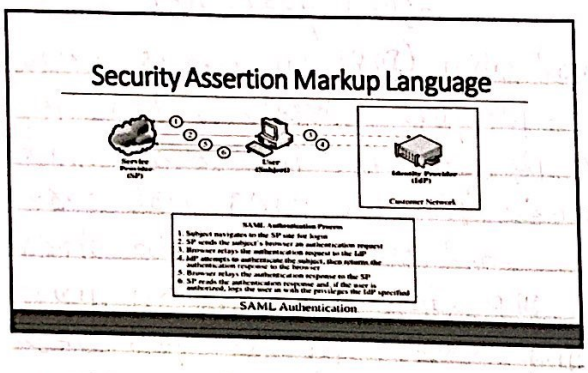
אבטחת יישומי ענן

בהשוואה הגבוהה ביותר שצריך לבצע בעת כתיבת יישומים לפריסה בענן היא להבין כיצד האיומים שלך משתנים.
ישנם כמה איומים כלליים הקיימים כתוצאה מהפרדיגמה מחשוב הענן:
- התקפות על משאבים משותפים.
- ממשקי API לא בטוחים.
למרבה הצער, קשה מדי לבצע אבטחה מקיפות של ספקי הענן והשותפים שלך, ולא ניתן לעשות הרבה כדי להגן על עצמך מפני סוגיות אלה.

Cloud Identity Management



ניהול זהויות ענן.



גרסת סימון קיצרת אפשרית