এডভান্স ডাটাবেস ম্যানেজমেন্ট সিস্টেম

বিষয় কোড - ৬৬৬৭৮ ৭ম পর্ব কম্পিউটার টেকনোলজি

ও এস পি এফ OSPF

আতিকুর রহমান
খন্ডকালিন শিক্ষক
ময়মনসিংহ পলিটেকনিক ইন্সটিটিউট
Email: atikcse@gmail.com

ডাটাবেস নরমালাইজেশন

ডাটাবেস নরমালাইজেশন

Normalization হল Database design করার এমন এক পদ্ধতি যা table decomposing এর মাধ্যমে database anomalies গুলিকে দূর করে এবং data-র প্রাচুর্য ও নির্ভরতা কমায় এবং good database তৈরী করতে সাহায্য করে।

ডাটাবেস নরমালাইজেশন কী? সর্বপ্রথম আসি, Normalization কি? কোন কিছুকে স্বাভাবিক অবস্থায় নিয়ে আসা। এখন ডাটাবেজের স্বাভাবিক অবস্থা বলতে, ডাটাবেজ থেকে প্রয়োজনের অতিরিক্ত জিনিস বাদ দেয়া যাকে ডাটা রিডানডেন্সি বলে এবং ডাটার বিশুদ্ধতা তৈরি করা যাকে ডাটা ইন্টিগ্রিটি ও বলা হয়। এখন Data Redundancy এবং Data Integrity কে উদাহরনসহ বর্ণনা করা যাক।

ডাটাবেস নরমালাইজেশন

ডাটা রিডানডেন্সি – আমরা যখন ডাটাবেজ ডিজাইন করি তখন অনেক সময় প্রয়োজনের অতিরিক্ত ডাটা জমা হয়। যাতে ডাটাবেজের মধ্যে একই ডাটা বার বার জমা হয়। এতে ডাটার রিডানডেন্সি বেড়ে যায়। এখন যদি ডাটাবেজকে নরমালাইজ করা হয় এতে অতিরিক্ত বা অপ্রয়োজনীয় ডাটা আর থাতে না।

ডাটা ইন্টিগ্রিটি – Data Integrity বলতে ডাটার বিশুদ্ধতা বুঝানো হয়েছে। এখন প্রশ্ন আসতে পারে ডাটার বিশুদ্ধতা কি? ধরি ডাটাবেজ এমনভাবে ডিজাইন করা হয়েছে যে, একজন ছাত্রের পরিক্ষার ফলাফল একেক জায়গায় একেক রকম। এক জায়গায় তার সর্বমোট নাম্বার ৪৭০, অন্য জায়গায় ৪৭৭। যা চুড়ান্ত ফলাফল তৈরিতে সমস্যার সৃষ্টি করবে। এই সমস্যার মাধ্যমে স্পষ্টত ডাটা তার শুদ্ধতা হারিয়েছে। এখন এই সমস্যা থেকে উত্তরণের একমাত্র উপায় হচ্ছে ডাটাবেজ নরমালাইজেশন। ডাটাবেজ নরমালাইজেশন করলে এই সমস্যা সমাধান করে একটি শুদ্ধ ডাটাবেজ তৈরি করা সম্ভব।

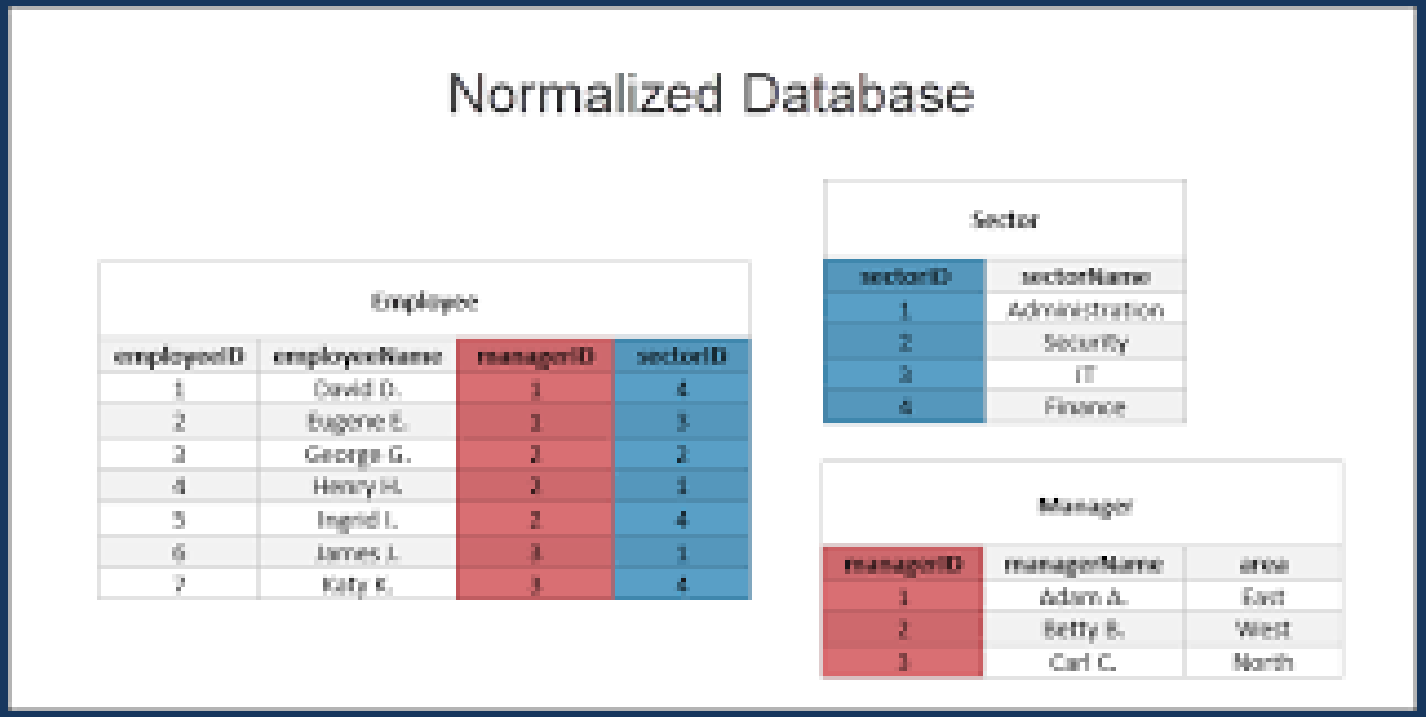


Figure: Database normalisation

প্রথম সাধারণ ফর্ম (1NF)

প্রথম সাধারণ ফর্মটি নির্দেশ করে যে আপনার ডাটাবেসের প্রতিটি ক্ষেত্রে শুধুমাত্র একটি মান সঞ্চয় করা উচিত এবং একটি ডাটাবেসে দুটি ক্ষেত্র থাকা উচিত নয় যা একইভাবে তথ্য সঞ্চয় করে। একটি উদাহরণ দিয়ে বিষয়টি আরও পরিষ্কার করা যাক। এটি এমন একটি ডাটাবেস যা কোর্স এবং তাদের পড়ান এমন অধ্যাপকদের তথ্য সংরক্ষণ করে।

প্রফেসর আইডি	অধ্যাপকের নাম	পাঠ্যধারাগুলি
P001	গ্রেগর মিচেল	সাহিত্য সৃজনশীল লেখা
P002	অ্যাঞ্জেলা ম্যাকগাল	পদার্থবিদ্যা

এই ডাটাবেস দুটি উপায়ে প্রথম স্বাভাবিক ফর্ম লঙ্ঘন করে:

প্রফেসর মিচেল দুটি কোর্স পড়ান থেকে একটি ক্ষেত্রে দুটি মান রয়েছে;
অনুরূপ তথ্য সংরক্ষণ করার দুটি ক্ষেত্র রয়েছে: অধ্যাপক আইডি এবং অধ্যাপকের নাম
উভয়ই অধ্যাপকের পরিচয় সম্পর্কিত তথ্য প্রদান করে।
আমাদের ডাটাবেস স্বাভাবিক করার জন্য, আমাদের এটি দুটি ভাগে বিভক্ত করতে হবে:

প্রথমটিতে অধ্যাপকদের পরিচয় সম্পর্কিত তথ্য থাকবে এবং এতে দুটি ক্ষেত্র, অধ্যাপক আইডি এবং অধ্যাপকের নাম অন্তর্ভুক্ত থাকবে।
দ্বিতীয়টির দুটি ক্ষেত্র থাকবে: একটি কোর্সের জন্য এবং একটি প্রফেসর আইডির জন্য যিনি সেই কোর্সটি শেখান সেই অধ্যাপকের সাথে সম্পর্কিত।

দ্বিতীয় সাধারণ ফর্ম (2NF)

দ্বিতীয় স্বাভাবিক ফর্মের লক্ষ্য হল অপ্রয়োজনীয়তা হ্রাস করা, নিশ্চিত করা যে প্রতিটি ক্ষেত্র তথ্য সঞ্চয় করে যা আমাদের প্রাথমিক কী সম্পর্কে কিছু বলে। অন্য কথায়:
প্রতিটি ডাটাবেসের শুধুমাত্র একটি প্রাথমিক কী থাকতে হবে
সমস্ত নন-প্রাথমিক কীগুলিকে প্রাথমিক কী-এর উপর সম্পূর্ণরূপে নির্ভর করতে হবে
এই দুটি নীতি নিশ্চিত করে যে প্রতিটি ডাটাবেস প্রাথমিক কী-তে থাকা একই যুক্তি সম্পর্কে সামঞ্জস্যপূর্ণ তথ্য সংরক্ষণ করে। আবার, আসুন একটি উদাহরণ দিয়ে আমাদের বোঝার সাহায্য করি।

অধ্যাপকের নাম	জন্মদিন	বিভাগ
হ্যারি গ্রে	জুলাই 1	সাহিত্য
ভিক্টোরিয়া হোয়াইট	সেপ্টেম্বর, ১৯	সাহিত্য
পল শৌল	1 মার্চ	সাহিত্য
জেমস স্মিথ	জুন, 5	বিজ্ঞান

উপরের ডাটাবেসটি প্রথম স্বাভাবিক ফর্ম অনুসরণ করে কারণ প্রতিটি ফিল্ডে তথ্যের একটিটুকরো থাকে এবং ক্ষেত্রগুলি বিভিন্ন তথ্য প্রদান করে। যাইহোক, এটি দ্বিতীয় স্বাভাবিক মাত্র ফর্মটিকে সম্মান করে না কারণ, যদিও জন্মদিনের ক্ষেত্রটি সম্পূর্ণরূপে তাদের নামের উপর নির্ভর করে, তারা যে বিভাগে অন্তর্ভুক্ত তা তাদের জন্মদিনের উপর নির্ভর করে না।

এই ডাটাবেসটিকে স্বাভাবিক করার জন্য, আবার, আমাদের এটিকে দুটি ভাগে ভাগ করতে হবে:

একটি অধ্যাপকের জন্মদিনের ডাটাবেস যা দুটি ক্ষেত্র অন্তর্ভুক্ত করে: অধ্যাপকের নাম এবং জন্মদিন

একটি অধ্যাপক বিভাগের ডাটাবেস যা দুটি ক্ষেত্র অন্তর্ভুক্ত করে: অধ্যাপকের নাম এবং বিভাগ

তৃতীয় সাধারণ ফর্ম (3NF)

একটি ডাটাবেস তৃতীয় স্বাভাবিক ফর্মকে সম্মান করে যখন এটির কোনো ট্রানজিটিভ নির্ভরতা থাকে না। একটি ট্রানজিটিভ নির্ভরতা কি? আপনার ট্রানজিটিভ নির্ভরতা থাকে যখন আপনার ডাটাবেসের কলাম B কলাম A নির্ভর করে, যা প্রাথমিক কী এর উপর নির্ভর করে।

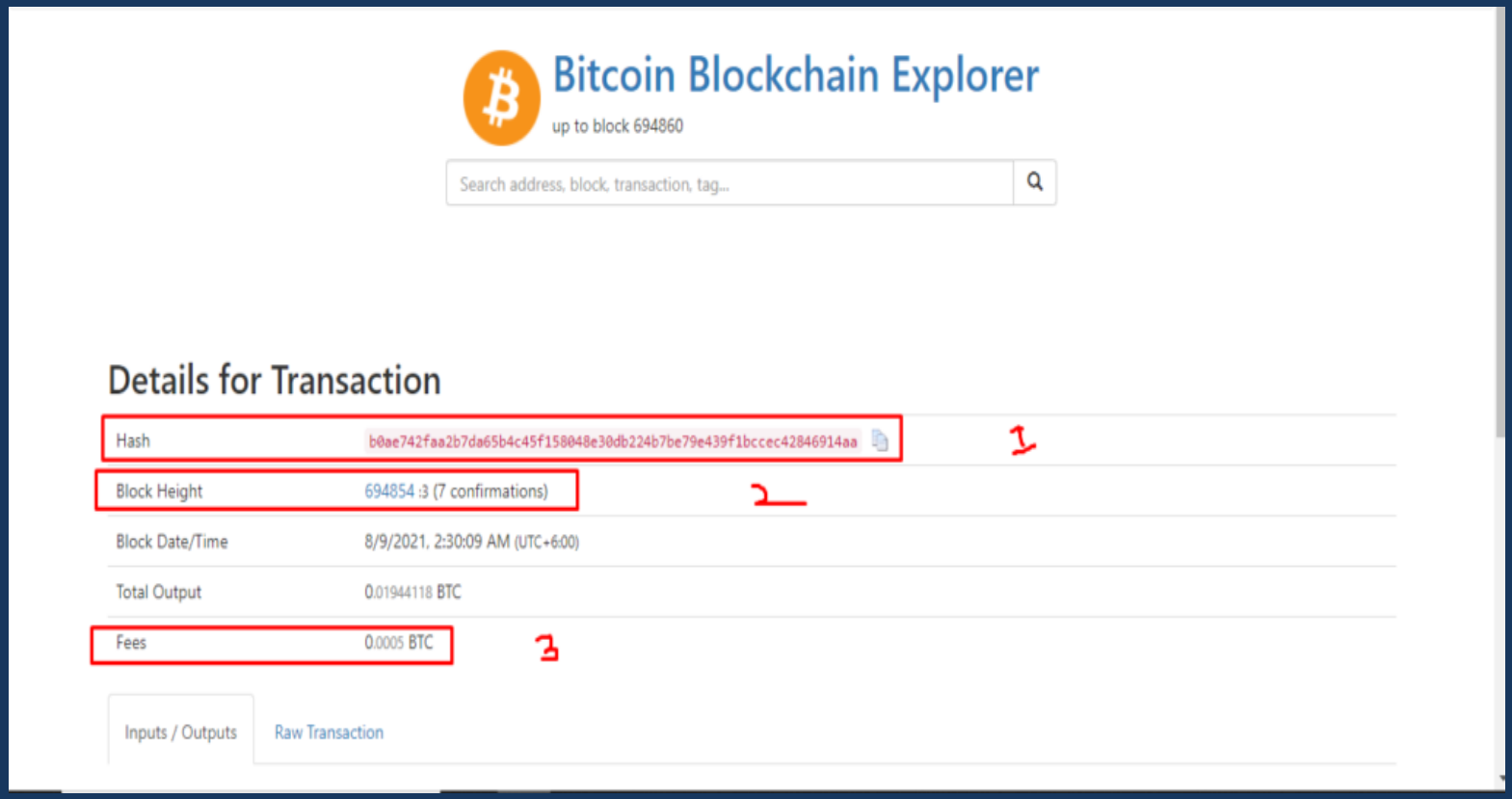
অর্ডার আইডি	অর্ডারের তারিখ	গ্রাহক আইডি	গ্রাহক জিপ কোড
D001	01/3/2022	C001	97438
D002	06/15/2022	C002	08638

এই ডাটাবেস তৃতীয় সাধারণ ফর্মটিকে সম্মান করে না কারণ আমাদের কাছে প্রাথমিক কী, অর্ডার আইডি রয়েছে। অর্ডারের তারিখ এবং গ্রাহক আইডি সম্পূর্ণরূপে এর উপর নির্ভরশীল, কিন্তু গ্রাহক জিপ কোড গ্রাহক আইডির উপর নির্ভর করে, যা প্রাথমিক কী নয়। আমরা যেমন উল্লেখ করেছি, তৃতীয় স্বাভাবিক ফর্ম অনুযায়ী এই ডাটাবেসটিকে স্বাভাবিক করার জন্য আমাদের একটি দ্বিতীয় গ্রাহক জিপ কোড ডেটাবেস তৈরি করতে হবে যা প্রতিটি গ্রাহক আইডিকে তাদের গ্রাহক জিপ কোডের সাথে সংযুক্ত করে।

ট্রানজেকশন এবং কনকারেন্সি কন্টোল অনুধাবন

Transaction বলতে কোন অর্থ বা তথ্যকে একস্থান থেকে অন্য স্থান এ স্থানান্তর করাকে বা পাঠানোকে বুঝানো হয়। ক্রিপ্টোকারেন্সি মার্কেটে ট্রান্সসেকশন বলতে যেকোনো কয়েন বা কারেন্সি এক ইউজার থেকে অন্য ইউজার এর কাছে আরো সুস্পষ্ট ভাবে বলতে গেলে এক অ্যাড্রেস থেকে অন্য অ্যাড্রেস এ পাঠানোকে বুঝায়।
ট্রান্সেকশন ব্লকচেইন এর মূল বৈশিষ্ট্যগুলোর মধ্যে একটা। ব্লকচেইন মুলত এই ট্রান্সেকশনের তথ্যকেই ব্লক আকারে নিজের মধ্যে অর্থাৎ ব্লকচেইনে ষ্টোর করে থাকে। তাই ব্লকচেইন সংক্রান্ত কাজ করতে হলে ট্রান্সেকশন সম্পর্কে ভালো ধারনা থাকা আবশ্যক।

প্রতি মিনিটে বর্তমানে প্রায় ৪৫০ এর উপর ট্রান্সেকশন হয়ে থাকে বিটকয়েন এর ব্লকচেইনে। কখনো কখনো এর সংখ্যা কয়েক হাজার ও ছাড়িয়ে যায়। বর্তমানে প্রায় ৭০০০ এর উপর কারেন্সি আছে মার্কেটে। তাদের সহ হিসাব করতে গেলে এই সংখ্যা লাখের উপর চলে যাবে। এখানে অপ্রাসঙ্গিক হলেও বলা উচিত যে, মিনিটে ট্রান্সেকশন এর পরিমান যত বেশি হয় তার উপর ভিত্তি করে ট্রান্সেকশন ফী পরিবর্তন হয়ে থাকে। ব্যাক্তিগত ওয়ালেট ব্যবহার করলে এই ফী এর ব্যাপারে ধারনা থাকা আবশ্যক। যদি অন্য মাধ্যম যেমন কোন এক্সচেঞ্জ বা 3rd Party Wallet ব্যবহার করা হলে সেখানে ফী নির্ধারন করা থাকে আগে থেকেই। ফলে তা ট্রান্সেকশন এর পরিমান এর উপর নির্ভর করে না।


Bitcoin Blockchain Explorer
up to block 694860
Search address, block, transaction, tag...
Details for Transaction
Hash
b0ae742faa2b7da65b4c45f158048e30db224b7be79e439f1bccec42846914aa
Block Height
694854 :3 (7 confirmations)
Block Date/Time
8/9/2021, 2:30:09 AM (UTC+6:00)
Total Output
0.01944118 BTC
Fees
0.0005 BTC
Inputs / Outputs
Raw Transaction
1
2
3

১. TxID: কোন ট্রান্সেকশন এর মূল জিনিসই হল ট্রান্সেকশন আইডি। এটা ছাড়া বা এটা ভুল হলে সেই ট্রান্সেকশনকে কোন ভাবেই ট্র্যাক করা সম্ভব না ব্লকচেইন এ । যদিও অন্য উপায় ব্যবহার করে অনেক সময় মিসিং ট্রান্সেকশন খুজে বের করা যায় তবে তা এখানে আলোচনা করার বিষয় না। আপনাকে মনে রাখতে হবে যে ট্রান্সেকশন আইডি ই ট্রান্সেকশন এর মূল জিনিস। ট্রান্সেকশন আইডি কে TxID বা Hash বা Transaction Hash বলা হয়ে থাকে অনেক সময়। নাম ভিন্ন হলেও একই জিনিসকে বুঝানো হয়ে থাকে।

২. Height বা Block Height: Height বলতে ব্লক হাইট কে বুঝানো হয়। ব্লক হাইট হল ব্লকচেইনের কত নাম্বার ব্লকে ট্রান্সেকশনটি কনফার্ম হয়েছে সেটা বুঝানো হয়। এই ব্লক হাইট থেকে বর্তমান সর্বশেষ ব্লক এর নাম্বার বাদ দিলে কনফার্মেশনের পরিমান জানা যায়।

৩. Fees: ফী বলতে বুঝানো হয় যে, ট্রান্সেকশনটি করতে কত পরিমানে কয়েন মাইনারকে ফী হিসাবে দেওয়া হয়েছে। এই ফী এর উপর ভিত্তি করে কনফার্মেশন দ্রুত বা দেরিতে হয়ে থাকে। ফী পর্যাপ্ত না হলে ট্রান্সেকশন কনফার্ম হতে দেরী হয়।

৪. Number of Confirmations: এর দ্বারা বুঝানো হয় যে, মোট কত ব্লক আগে ট্রান্সেকশনটি কনফার্ম হয়েছে। এটা অত্যন্ত গুরুত্বপূর্ণ বিষয়। কারন প্রতি এক্সচেঞ্জ এ প্রতি কয়েনের জন্য আলাদা আলাদা কনফার্মেশন নাম্বার থাকে। তাই কতটা সময় লাগবে এক্সচেঞ্জ এ কয়েন অ্যাড হতে তা এই কনফার্মেশন নাম্বার থেকে বুঝা যায়।

৫. Input/Output: Input দিয়ে বুঝানো হয় কোন কোন অ্যাড্রেস হতে কত পরিমানে কয়েন ট্রান্সেকশন এ নেওয়া হয়েছে এবং Output বলতে বুঝানো হয় মোট কত পরিমানে কয়েন কোন কোন অ্যাড্রেস এ সেন্ড করা হয়েছে।

৬. Status: Status ৩ রকমের হয় সাধারনত। Pending, Unconfirmed এবং Confirmed

ডাটাবেজ সিকিউরিটি

ডেটাবেস নিরাপত্তা বলতে নিয়ন্ত্রণ, সরঞ্জাম, নীতি এবং ডেটার গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা, সেইসাথে ডেটা ম্যানেজমেন্ট সিস্টেম এবং এটি অ্যাক্সেস করা অ্যাপ্লিকেশনগুলিকে সংরক্ষণ করার জন্য ডিজাইন করা অন্যান্য ব্যবস্থা বোঝায়।

ডাটাবেস নিরাপত্তা কেন গুরুত্বপূর্ণ?

ডাটাবেস নিরাপত্তার গুরুত্বের জন্য উদ্ধৃত শীর্ষ কারণ হল ডেটা লঙ্ঘনের ঝুঁকি হ্রাস করা। সাম্প্রতিক তথ্য অনুসারে, ডেটা লঙ্ঘনের গড় খরচ এখন $৪.২৪ মিলিয়ন, আগের বছরের তুলনায় একটি বিশাল ১০% বৃদ্ধি – এবং এমনকি বেশি যেখানে দূরবর্তী কাজ একটি ফ্যাক্টর ছিল। যাইহোক, ডাটাবেস নিরাপত্তার জন্য অনেক কারণ রয়েছে, যার মধ্যে রয়েছে:

প্রটেকশন অফ ইন্টেলেকচুয়াল প্রপার্টি (আইপি) অপসারণ বা ক্ষতির বিরুদ্ধে (যেমন হার্ডওয়্যার ব্যর্থতা), যা প্রতিযোগিতা করার ক্ষমতাকে প্রভাবিত করতে পারে।

ডেটা লঙ্ঘন প্রতিরোধ করুন, যা প্রকৃত ডলারে (নিয়ন্ত্রক সম্মতি জরিমানা, আইনী ফি, লঙ্ঘনের বিজ্ঞপ্তি খরচ) এবং ব্র্যান্ডের খ্যাতি উভয় ক্ষেত্রেই উচ্চ খরচ বহন করে।

IP হারানো বা উচ্চ লঙ্ঘনের খরচের কারণে ব্যবসার ধারাবাহিকতা। অনেক ছোট থেকে মাঝারি আকারের ব্যবসা বন্ধ হয়ে যাবে যদি তারা লঙ্ঘনের সম্মুখীন হয়।

ডেটা অখণ্ডতা বজায় রাখতে এবং ব্যবহারকারীর ভুলে যাওয়ার অধিকারকে সমর্থন করার জন্য নিয়ন্ত্রক সম্মতির প্রয়োজনীয়তা।

যেসব ব্যবসার ডেটাবেস নিরাপত্তার প্রয়োজন সবচেয়ে বেশি

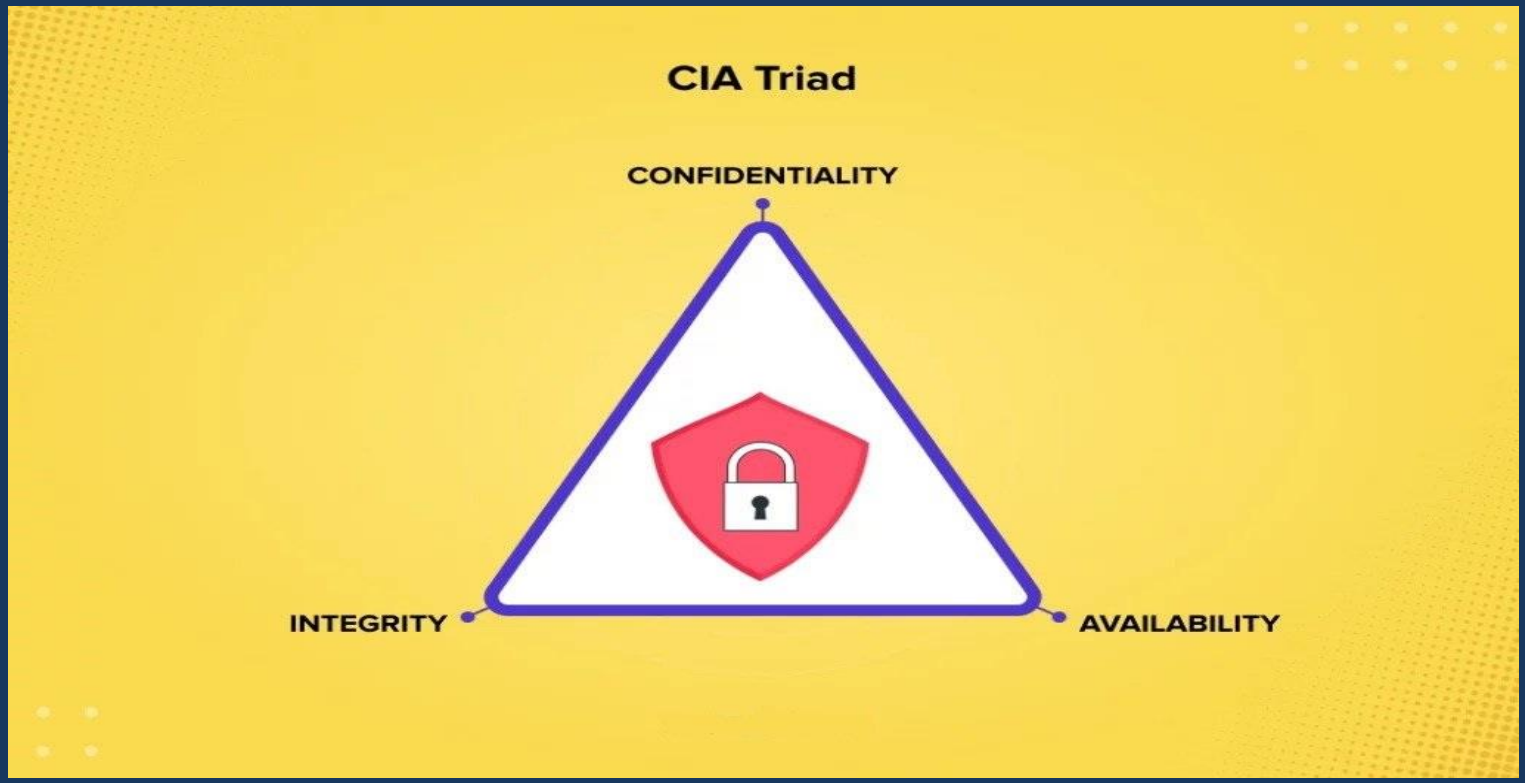
সাইবার ক্রাইম বৈষম্য করে না, সমস্ত আকারের সমস্ত শিল্প এবং ব্যবসায় আক্রমণ করে। যদিও এটি সত্য, কিছু শিল্প অন্যদের তুলনায় বেশি টার্গেট করা হয় – যে শিল্পগুলির ডেটা কালো বাজারে বেশি মূল্যের হতে পারে, তারা সাইবার গুপ্তচরবৃত্তির লক্ষ্য, বা যাদের সুরক্ষা দুর্বল হিসাবে বিবেচিত হতে পারে।

১. স্বাস্থ্যসেবা

রোগীর তথ্য কালোবাজারে বেশি মূল্যবান, ক্রেডিট কার্ডের ডেটার চেয়ে অন্তত ১০ গুণ বেশি মূল্যবান, স্বাস্থ্যসেবা সাইবার আক্রমণের জন্য সবচেয়ে বেশি টার্গেট করা শিল্প। একীভূতকরণ এবং অধিগ্রহণের প্রবণতা এবং ঘূর্ণায়মান এবং চুক্তি কর্মীদের জন্য ডেটা অ্যাক্সেস পরিচালনার জটিলতার সাথে মিলিত উত্তরাধিকার এবং নতুন চিকিৎসা ডিভাইসের একটি জটিল মিশ্রণ, ফাঁকগুলি উপেক্ষা করার ঝুঁকি বাড়ায়।

২. সরকার ও সমালোচনামূলক অবকাঠামো

গত দুই বছরে, জাতি রাষ্ট্র আক্রমণকারীদের দ্বারা সংঘটিত আক্রমণের দিকে একটি প্রবণতা রয়েছে যারা আর্থিক লাভের পাশাপাশি সাইবার গুপ্তচরবৃত্তি (গুপ্তচরবৃত্তি) কার্যকলাপে ব্যাঘাত ও ধ্বংস বা অংশ নেওয়ার ইচ্ছা দ্বারা অনুপ্রাণিত। ২০২০-তে, ১৩% দূষিত লঙ্ঘন হয়েছিল জাতি রাষ্ট্র আক্রমণকারীদের দ্বারা।



৩. অর্থনৈতিক সেবা সমূহ

স্বাস্থ্যসেবার পিছনে, আর্থিক পরিষেবাগুলি ডেটা লঙ্ঘনের সর্বোচ্চ ব্যয় এবং আক্রমণের সর্বোচ্চ হারগুলির মধ্যে একটির মুখোমুখি হয়। প্রকৃতপক্ষে, অর্থের উপর ২৮% আক্রমণ ছিল সার্ভার অ্যাক্সেস আক্রমণ।

৪. খুচরা এবং ইকমার্স

ডাটাবেসে সংরক্ষিত উচ্চ মূল্যের আর্থিক এবং ব্যক্তিগত বিবরণের কারণে সমস্ত আক্রমণের অন্তত ১০.২% খুচরা শিল্পকে লক্ষ্য করে।

ডাটাবেস নিরাপত্তা হুমকি এবং দুর্বলতা

সবচেয়ে সাধারণ ডাটাবেস নিরাপত্তা দুর্বলতা, হুমকি এবং চ্যালেঞ্জ অন্তর্ভুক্ত:

১. ভিতরের হুমকি

এগুলি সিস্টেম এবং ডেটাতে অভ্যন্তরীণ অ্যাক্সেস রয়েছে এমন ব্যক্তিদের থেকে ঝুঁকি, যার মধ্যে বর্তমান কর্মচারীদের পাশাপাশি অতীতের কর্মচারী (অধিকৃত অ্যাক্সেস সহ) বা তৃতীয় পক্ষের অংশীদার বা ঠিকাদার অন্তর্ভুক্ত থাকতে পারে। অভ্যন্তরীণ হুমকিগুলি গত দুই বছরে ৪৪% বেড়েছে এবং ঘটনা প্রতি খরচ হয়েছে $১৫.৩৮ মিলিয়ন। ক্ষতিকারক অভ্যন্তরীণ হুমকিগুলিও ক্রমবর্ধমানভাবে ডাটাবেস ব্যাকআপগুলিকে লক্ষ্যবস্তু করছে।

অভ্যন্তরীণ হুমকি উভয়ই বিদ্বেষপূর্ণ হতে পারে (যারা লাভ বা প্রতিশোধের জন্য ক্ষতি করতে চায় তাদের কাছ থেকে) এবং অবহেলা (যারা ঝুঁকির পরিচয় দেয় এমন ভুল করে)। আপোসকৃত শংসাপত্রের ব্যবহার একটি অভ্যন্তরীণ হুমকিও গঠন করে, বাইরের আক্রমণকারী ফিশিং বা শংসাপত্র ডাটাবেসের আপসের মাধ্যমে শংসাপত্রগুলিতে অ্যাক্সেস লাভ করে।

২. মানুষের ত্রুটি

মানবিক ত্রুটি হল গুরুতর ডেটা লঙ্ঘনের প্রধান কারণ, যা নিরাপত্তার ঘটনাগুলির ৮৪% এর সাথে যুক্ত, বিশেষ মনোযোগের যোগ্য। সবচেয়ে সাধারণ মানবিক ত্রুটিগুলির মধ্যে রয়েছে: ফিশিং লিঙ্কে ক্লিক করা, দুর্বল পাসওয়ার্ড স্বাস্থ্যবিধি, পাসওয়ার্ড ভাগ করে নেওয়া, প্যাচিং উপেক্ষা করা, এবং অন্য উত্সে (যেমন ক্লাউড অ্যাপ্লিকেশন, ইমেল) নিরাপদ ডেটার অননুমোদিত বহিষ্কার। মানব ত্রুটি শারীরিক নিরাপত্তার সাথে আপস করতে পারে, যেমন কাউকে প্রমাণীকরণ ছাড়া একটি নিরাপদ এলাকায় হাঁটার অনুমতি দেয়।

৩. সাইবার হামলা

সাইবার আক্রমণ অনেক রূপে আসে, কিন্তু ডাটাবেস নিরাপত্তার সবচেয়ে সাধারণ আক্রমণ এবং শোষণের মধ্যে রয়েছে:

ক. ডাটাবেস সফ্টওয়্যার দুর্বলতা

ডাটাবেস ম্যানেজমেন্ট প্ল্যাটফর্ম, নেটওয়ার্ক বা এই সিস্টেমগুলি অ্যাক্সেস করার জন্য ব্যবহৃত অ্যাপ্লিকেশনগুলি সহ সমস্ত সফ্টওয়্যারের জন্য দুর্বলতাগুলি সাধারণ। নিয়মিত প্যাচিং ছাড়া, এই দুর্বলতাগুলি আক্রমণের জন্য সিস্টেমগুলিকে উন্মুক্ত করে দেয়।

খ. SQL/NoSQL ইনজেকশন আক্রমণ

সমস্ত ডাটাবেস সিস্টেম এই ধরণের আক্রমণের জন্য ঝুঁকিপূর্ণ, যা আক্রমণকারীদের ডাটাবেসে কমান্ড কার্যকর করতে বা ডাটাবেসের জন্য কমান্ডগুলিতে কোড ইনজেক্ট করতে দেয়।

গ. পরিষেবা অস্বীকার (DoS/DDoS) আক্রমণ

আক্রমণগুলি একটি মেশিন বা নেটওয়ার্ক বন্ধ করে দেয়, যা ডাটাবেস অ্যাক্সেস করা অসম্ভব করে তোলে। সবচেয়ে সাধারণ DoS আক্রমণ হল একটি বাফার ওভারফ্লো আক্রমণ, যা পরিচালনার জন্য ডিজাইন করা সিস্টেমের চেয়ে বেশি ট্রাফিক পাঠায়।

ক. ডাটাবেস সফ্টওয়্যার দুর্বলতা

ডাটাবেস ম্যানেজমেন্ট প্ল্যাটফর্ম, নেটওয়ার্ক বা এই সিস্টেমগুলি অ্যাক্সেস করার জন্য ব্যবহৃত অ্যাপ্লিকেশনগুলি সহ সমস্ত সফ্টওয়্যারের জন্য দুর্বলতাগুলি সাধারণ। নিয়মিত প্যাচিং ছাড়া, এই দুর্বলতাগুলি আক্রমণের জন্য সিস্টেমগুলিকে উন্মুক্ত করে দেয়।

খ. SQL/NoSQL ইনজেকশন আক্রমণ

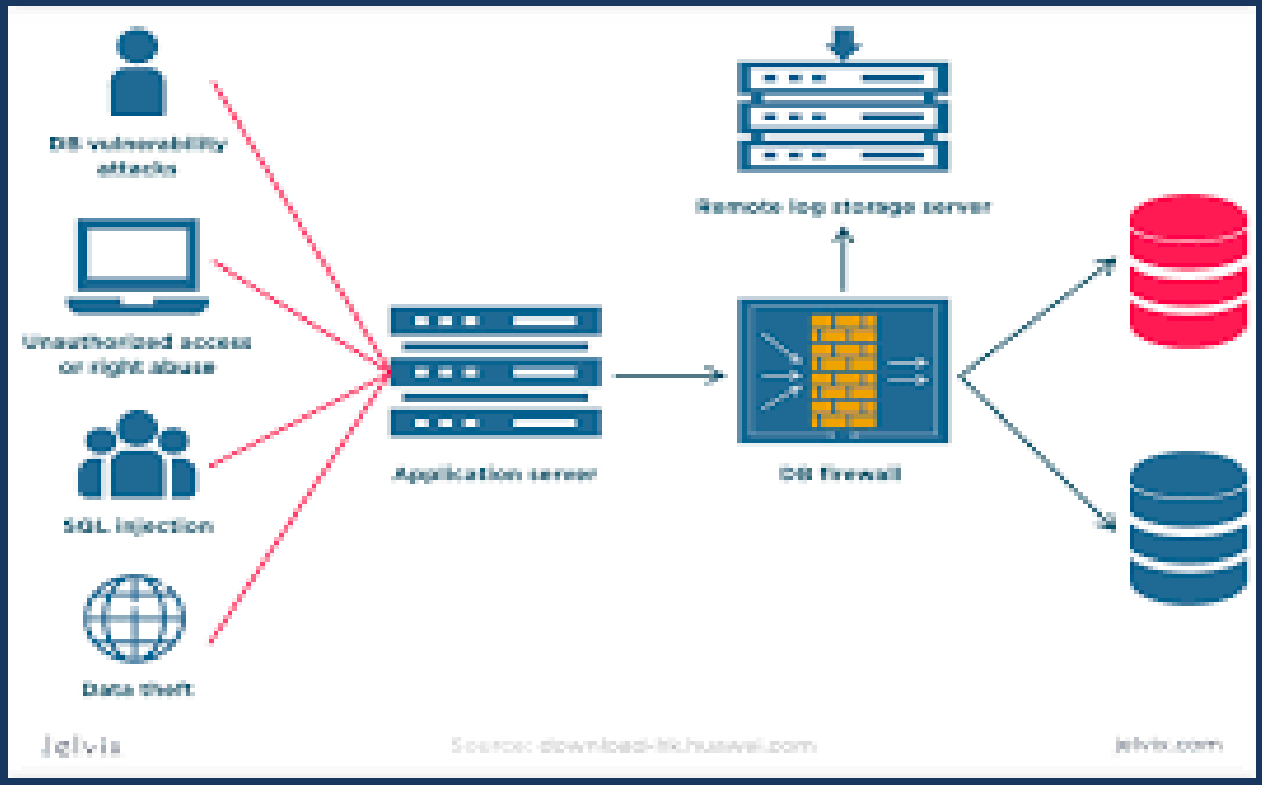
সমস্ত ডাটাবেস সিস্টেম এই ধরণের আক্রমণের জন্য ঝুঁকিপূর্ণ, যা আক্রমণকারীদের ডাটাবেসে কমান্ড কার্যকর করতে বা ডাটাবেসের জন্য কমান্ডগুলিতে কোড ইনজেক্ট করতে দেয়।

গ. পরিষেবা অস্বীকার (DoS/DDoS) আক্রমণ

আক্রমণগুলি একটি মেশিন বা নেটওয়ার্ক বন্ধ করে দেয়, যা ডাটাবেস অ্যাক্সেস করা অসম্ভব করে তোলে। সবচেয়ে সাধারণ DoS আক্রমণ হল একটি বাফার ওভারফ্লো আক্রমণ, যা পরিচালনার জন্য ডিজাইন করা সিস্টেমের চেয়ে বেশি ট্রাফিক পাঠায়।

ঘ. ম্যালওয়্যার

ক্ষতিকারক সফ্টওয়্যার (ম্যালওয়্যার) হল এমন সফ্টওয়্যার যা ডেটা চুরি করতে, সিস্টেমকে ব্যাহত করতে বা ক্ষতি করার জন্য টার্গেট সিস্টেমে অনুপ্রবেশ করার জন্য ডিজাইন করা হয়েছে। ম্যালওয়্যারের সবচেয়ে সাধারণ বিপজ্জনক প্রকারগুলি হল র্যানসমওয়্যার (যেখানে অপরাধীরা তথ্য এনক্রিপ্ট করে এবং অর্থ প্রদানের দাবি করে) বা শূন্য-দিনের আক্রমণ, যা বিক্রেতা সচেতন হওয়ার আগেই ডাটাবেস সফ্টওয়্যার দুর্বলতাগুলিকে কাজে লাগায়।


DB vulnerability attacks
Unauthorized access or right abuse
SQL injection
Data theft
Application server
Remote log storage server
DB firewall
jelvis
jelvis.com

৪. আইটি পরিবেশের চাপ

পরিবর্তনশীল আইটি পরিবেশ বিদ্যমান ডাটাবেসের পাশাপাশি ডাটাবেস সুরক্ষা অনুশীলন এবং সরঞ্জামগুলির উপর চাপ সৃষ্টি করছে, যার সবগুলি গতিশীল নয়। আইটি পরিবেশে কিছু শীর্ষ চাপের মধ্যে রয়েছে:

ক. ডেটা ভলিউম

'বিগ ডেটা'-এর বৃদ্ধি কীভাবে ডেটা ক্যাপচার করা, সংরক্ষণ করা, প্রক্রিয়া করা এবং ব্যাক আপ করা হয় তার উপর নতুন চাপ তৈরি করে। সমস্ত সিস্টেম এবং প্রক্রিয়াগুলি ভালভাবে স্কেল করা হয় না, যার ফলে ধীর সিস্টেম, ঝুঁকি এবং ক্রমবর্ধমান ত্রুটি হয়।

খ. বিতরণ করা অবকাঠামো

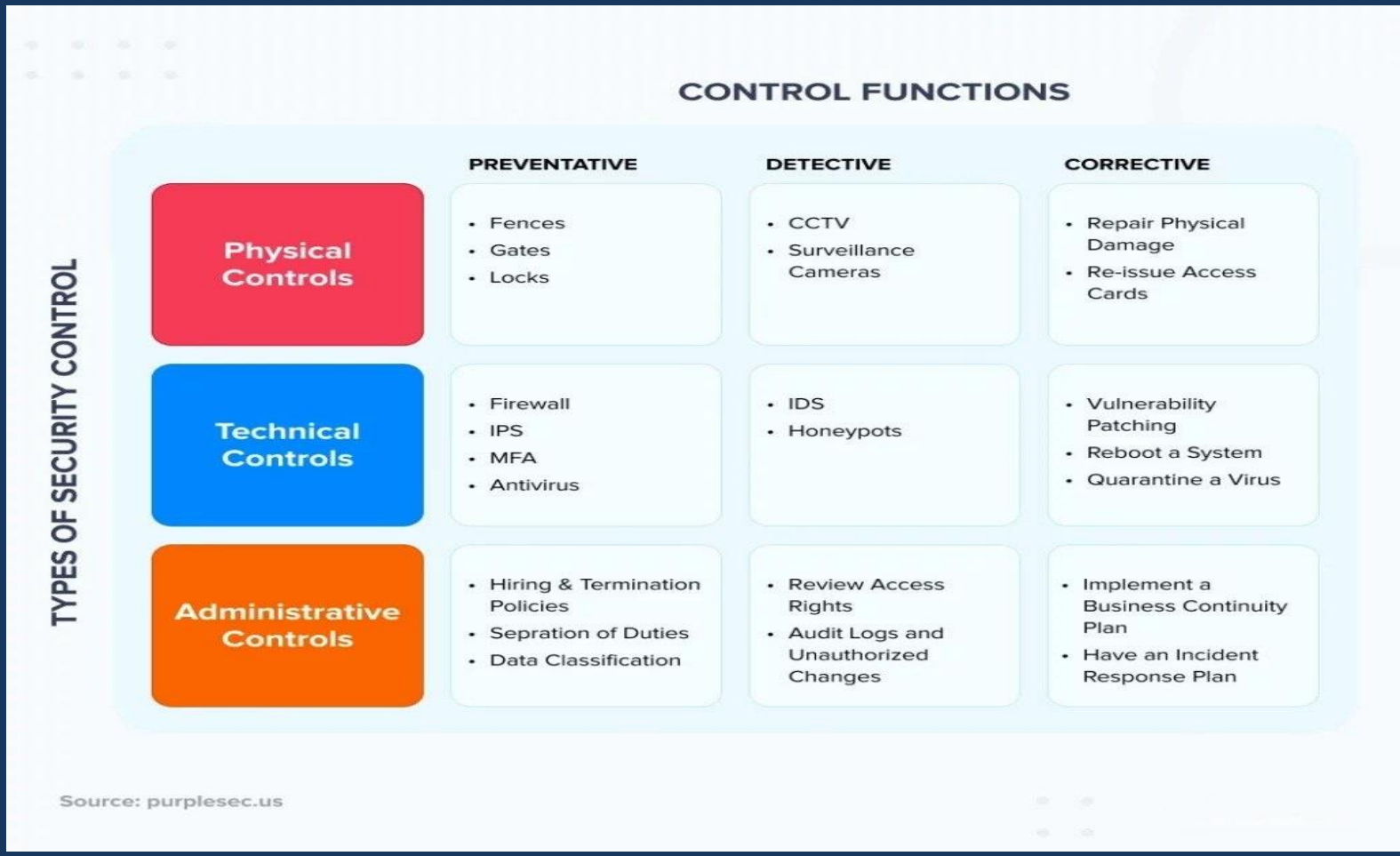
যেহেতু সংস্থাগুলি ক্রমবর্ধমানভাবে ক্লাউড অবকাঠামো এবং মাইক্রোসার্ভিস আর্কিটেকচার গ্রহণ করছে, ডাটাবেস সুরক্ষা চ্যালেঞ্জগুলি দ্রুতগতিতে আরও জটিল হয়ে উঠেছে।

গ. নিয়ন্ত্রক প্রয়োজনীয়তা

রাজ্য, ফেডারেল, শিল্প এবং বৈশ্বিক স্তরে নিয়ন্ত্রক পরিবেশ দ্রুত পরিবর্তিত হচ্ছে, এখন ডাটাবেস সুরক্ষা থেকে আরও বেশি প্রয়োজন (যেমন ডেটা অখণ্ডতা, ভুলে যাওয়ার অধিকার), যা কিছু সিস্টেম পরিচালনা করতে পারে না।

ঘ. আইটি দক্ষতার অভাব

মার্কিন যুক্তরাষ্ট্রে আইটি দক্ষতার ঘাটতি, বিশেষ করে সাইবার নিরাপত্তায়, অনেক সংস্থার জন্য ডাটাবেস নিরাপত্তার পরিবর্তনশীল চাহিদাগুলি মেনে চলা কঠিন করে তোলে।



ডেটাবেস নিরাপত্তা সর্বোত্তম অভ্যাস

তিন ধরনের ডাটাবেস নিরাপত্তা নিয়ন্ত্রণের মধ্যে (ভৌত, প্রযুক্তিগত, প্রশাসনিক), অনেকগুলি নির্দিষ্ট স্তর রয়েছে। এই স্তরগুলি একটি নির্দিষ্ট আইটি পরিবেশের মধ্যে ডাটাবেসের নকশা, স্থাপনা এবং চলমান ব্যবহার সম্পর্কে অবহিত করতে সহায়তা করে।

১. শারীরিক নিরাপত্তা

নিশ্চিত করুন যে ডাটাবেস সার্ভারটি সুরক্ষিত আছে, সাইটটিতে হোক বা ক্লাউড ডেটা সেন্টারে, পর্যাপ্তভাবে পর্যবেক্ষণ করা এবং জলবায়ু-নিয়ন্ত্রিত একটি সুবিধায় শারীরিক অ্যাক্সেস ব্যবস্থা (যেমন কার্ড বা হার্ডওয়্যার-ভিত্তিক প্রমাণীকরণ প্রোটোকল) দ্বারা সুরক্ষিত। যারা ওয়েব হোস্টিং ব্যবহার করেন তাদের জন্য, ডাটাবেসের নিরাপত্তা নিশ্চিত করার জন্য যথাযথ পরিশ্রম করা উচিত।

২. প্যাচিং

যেকোন ডাটাবেস সিস্টেমে দুর্বলতার সবচেয়ে বড় ক্ষেত্রগুলির মধ্যে একটি হল ডাটাবেস সার্ভারের কার্যকর প্যাচ ব্যবস্থাপনার অভাব এবং নেটওয়ার্কের সাথে সংযোগকারী অ্যাপ্লিকেশনগুলি নিয়মিতভাবে নতুন দুর্বলতা আবিষ্কৃত হয়। আরও, অনেক প্যাচ স্থিতিশীলতার সমস্যাগুলিকে মোকাবেলা করে, ডাটাবেস সিস্টেমের অখণ্ডতা এবং প্রাপ্যতা মোকাবেলায় সহায়তা করে।

৪. অ্যাক্সেস কন্ট্রোল এবং প্রমাণীকরণ

অ্যাক্সেস কন্ট্রোলগুলি নির্ধারণ করে যে কে একটি সিস্টেমে অ্যাক্সেস পায় এবং কী ক্ষমতায় – ডাটাবেস সিস্টেমে রিসোর্স পড়তে, তৈরি করতে, আপডেট করতে বা মুছতে পারে। প্রমাণীকরণ হল একটি ব্যবহারকারী যাচাই করার প্রক্রিয়া যা তারা বলে যে তারা।

ডাটাবেসের নিরাপত্তার জন্য, ব্যবহারকারীদের তাদের কাজ করার জন্য প্রয়োজনীয় ন্যূনতম সংখ্যক অনুমতি বরাদ্দ করা এবং অ্যাডমিন অ্যাকাউন্ট অ্যাক্সেস আলাদা করা এবং সর্বদা ব্যবহারকারীদের যাচাই করার জন্য "শূন্য বিশ্বাস" ধারণার সাথে সক্রিয়ভাবে অ্যাক্সেস নিয়ন্ত্রণগুলি পরিচালনা করা গুরুত্বপূর্ণ।

অ্যাক্সেস কন্ট্রোল এবং প্রমাণীকরণ চেকলিস্ট:

অ্যাক্সেস ম্যানেজমেন্টের জন্য মৌলিক নিয়ন্ত্রণ সেট আপ করুন

নীতিগুলি সেট আপ করুন যা ডাটাবেসে প্রশাসনিক বা বিশেষাধিকারপ্রাপ্ত অ্যাক্সেস পরিচালনা করে (ডাটাবেস ইনস্টল, পরিবর্তন, কনফিগার, মুছে ফেলা বা অন্যথায় পরিচালনা করতে)

বিশেষাধিকারপ্রাপ্ত ব্যবহার / সুবিধাপ্রাপ্ত ব্যবহারকারীদের জন্য উচ্চ স্তরের নিয়ন্ত্রণ বিবেচনা করুন (IAM, PAM)

প্রমাণীকরণ ফ্যাক্টর(গুলি) এবং প্রয়োজনীয় যেকোন প্রয়োগকরণ নির্ধারণ করুন (যেমন পাসওয়ার্ডের শক্তি, অ্যাকাউন্ট লক সেটিংস, সঞ্চিত পাসওয়ার্ডগুলির এনক্রিপশন)

উপসংহার

আজকের ডিজিটাল বিশ্ব ডাটাবেসের উপর অনেক বেশি নির্ভর করে, তাই আক্রমণের বিরুদ্ধে এই মূল্যবান সম্পদগুলিকে রক্ষা করা এবং সর্বদা ডেটার অখণ্ডতা এবং প্রাপ্যতা বজায় রাখা গুরুত্বপূর্ণ। যাইহোক, ডাটাবেস সুরক্ষার অনেকগুলি চলমান অংশ রয়েছে এবং, যেমনটি আগে বলা হয়েছে, অনেক সংস্থার পরিবর্তনশীল ঝুঁকির ল্যান্ডস্কেপের শীর্ষে থাকার জন্য পর্যাপ্ত অভ্যন্তরীণ দক্ষতার অভাব রয়েছে। আপনি একটি নতুন ক্লাউড পরিবেশে স্থানান্তরিত হচ্ছেন বা আপনার ডাটাবেস নিরাপত্তা ভঙ্গির একটি অডিট বা অপ্টিমাইজেশন খুঁজছেন কিনা, নেট সলিউশনের বিশেষজ্ঞ ডাটাবেস ডেভেলপার আছে আপনার প্রয়োজনের গভীরে ডুব দিতে।

১. ডাটাবেস নিরাপত্তার বিভিন্ন স্তর কি কি?

ডাটাবেস সুরক্ষার চারটি স্তর রয়েছে: সুরক্ষা স্তর, ডাটাবেস স্তর, অ্যাক্সেস স্তর এবং ঘের স্তর।

নিরাপত্তা স্তর ডাটাবেস নিরাপত্তা সমাধান নিয়ে কাজ করে।

ডাটাবেস স্তরে টোকেনাইজেশন, মাস্কিং এবং এনক্রিপশন জড়িত।

অ্যাক্সেস নিয়ন্ত্রণ তালিকা এবং অনুমতিগুলি অ্যাক্সেস স্তরের অংশ।

পারমিটার স্তরে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক এবং ফায়ারওয়াল অন্তর্ভুক্ত রয়েছে

৩. ডাটাবেস নিরাপত্তা পরীক্ষা বিভিন্ন ধরনের কি কি?

বিভিন্ন ধরনের ডাটাবেস নিরাপত্তা পরীক্ষা হল:

অনুপ্রবেশ পরীক্ষা: ইচ্ছাকৃতভাবে নিরাপত্তা ত্রুটিগুলি আবিষ্কার করার জন্য একটি সিস্টেম আক্রমণ.

ঝুঁকি মূল্যায়ন: আপনার ডাটাবেসের সাথে জড়িত ঝুঁকির মাত্রা নির্ধারণের জন্য একটি ঝুঁকি মূল্যায়ন পরিচালনা করা।

পাসওয়ার্ড ক্র্যাকিং: আপনার পাসওয়ার্ড হ্যাক হতে পারে কিনা তা দেখতে পাসওয়ার্ড-ক্র্যাকিং সরঞ্জাম ব্যবহার করে।

নিরাপত্তা নিরীক্ষা: সংস্থা নিরাপত্তা মান অনুসরণ করছে কি না তা দেখতে নিরাপত্তা নিরীক্ষা পরিচালনা করা।

- Thank You