

Secure-By-Design

Cultivating a Security-First Mindset

Sushma Singh



**Believe your business is
cyber-safe with just
firewalls and passwords?**



THINK AGAIN !





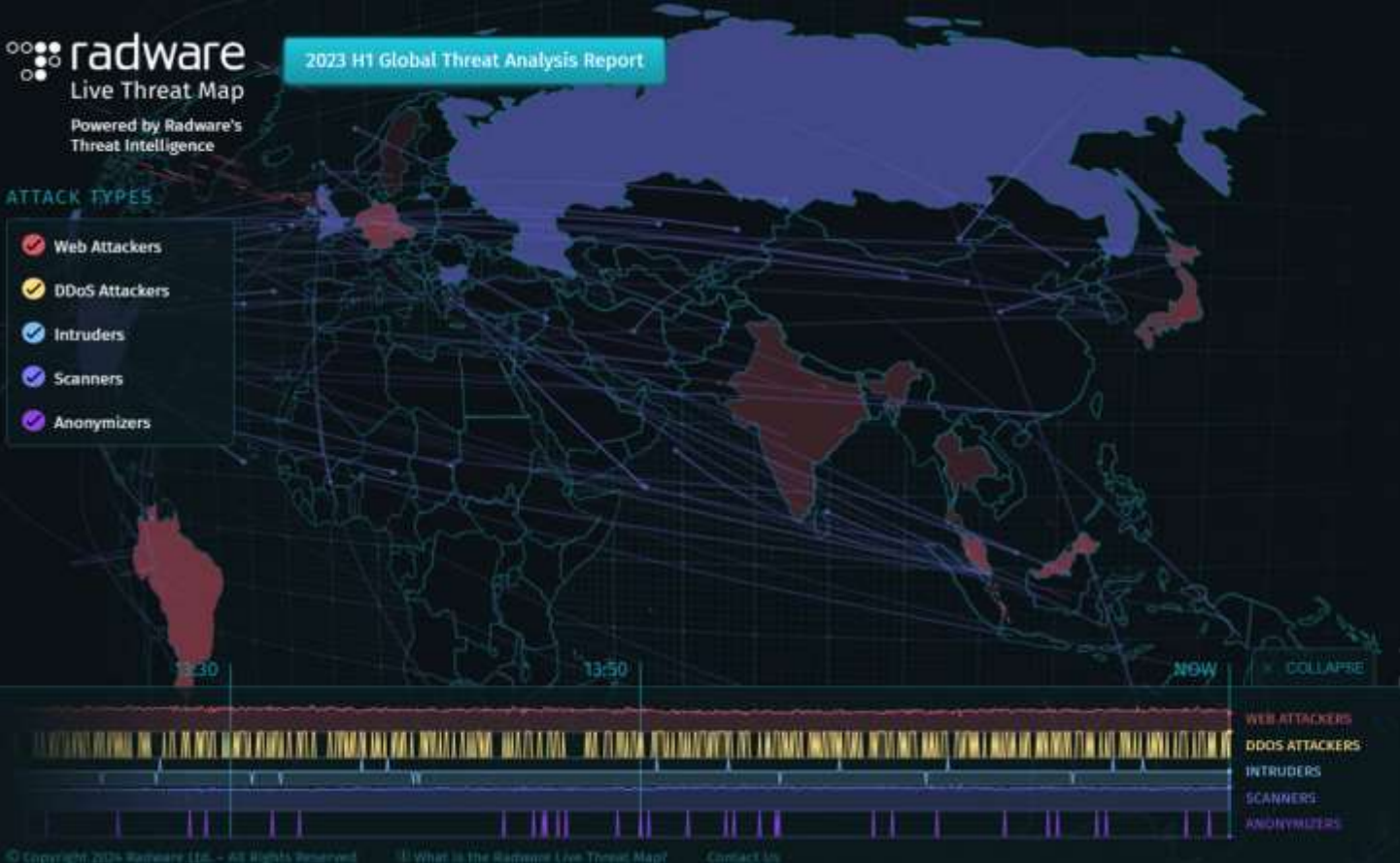
**By 2027, global cost
of cyber crime is
expected to reach
\$23.84 TRILLION.**



Source:
Statista's Cybersecurity Outlook

ATTACK TYPES

- Web Attackers
- DDoS Attackers
- Intruders
- Scanners
- Anonymizers



STATISTICS INTERVAL

1 hour

TOP ATTACKERS

United States	61 %
United Kingdom	13 %
Malaysia	10 %
Netherlands	9 %
China	7 %

TOP ATTACKED

United States	36 %
India	21 %
Japan	21 %
Korea	11 %
Indonesia	11 %

TOP NETWORK ATTACK VECTORS

TCP Flood	88 %
UDP Flood	7 %
IP Flood	3 %
DNS Flood	1 %
DoS	1 %

TOP APPLICATION VIOLATIONS

Access violations	52 %
Injections	23 %
Exploits	14 %
Cross-site scripting	6 %
Data theft	5 %

Don't take my word for it.

Here's A Glimpse...

...Decide For Yourself.



Network Vulnerability

Oct, 2023

***Aadhaar details of 81.5 cr people leaked
in India's 'biggest' data breach***



The Okta logo, consisting of the word "okta" in a bold, blue, lowercase sans-serif font, is centered within a white square.

**Phishing
& Supply
Chain**

Oct, 2023

Okta Breach Impacted All Customer Support Users—Not 1 Percent

Okta upped its original estimate of customer support users affected by a recent breach from 1 percent to 100 percent, citing a “discrepancy.”





**Social Engg
& Supply
Chain**

Oct, 2023

***Casino giant MGM expects \$100 million hit
from hack that led to data breach***





**SQL
Injection
& Supply
Chain**

May, 2023

The Biggest Hack of 2023 Keeps Getting Bigger

Victims of the MOVEit breach continue to come forward. But the full scale of the attack is still unknown.





**Password
Reuse**

Dec, 2023

Data Breach at 23andMe Affects 6.9 Million Profiles, Company Says

Hackers were able to obtain access because some customers reused old passwords, the genetic testing company said.





**Network &
Database**

Sept, 2023

Mixin halts withdrawals as network suffers

\$200M loss in hack

Attackers gained unauthorized access to the Mixin Network's cloud service provider's centralized database





**SIM Swap
& MFA**

Jan, 2024

Twitter: SEC's Account Was Hijacked Through a SIM-Swap Attack

Twitter also says @SECGov neglected to use two-factor authentication.





Nov 2022

AIIMS Delhi: Held to ransom by cyber attack

The perpetrators held around 4 crore patient profiles at ransom – including sensitive data and medical records of VIPs.





**Zero Day
& DDOS**

Dec, 2023

***Cloudflare, Google, and Amazon explain
what's behind the largest DDoS attacks
ever***





Jan, 2024

***Microsoft breached by Russian APT
behind SolarWinds attack***

Several email accounts belonging to Microsoft senior leadership were accessed as part of the breach, though Microsoft found 'no evidence' of customer environments being accessed.





**Exposure
Mishap**

Mar, 2023

GitHub's Private RSA SSH Key Mistakenly Exposed in Public Repository

GitHub hastens to replace its RSA SSH host key after an exposure mishap threatens users with man-in-the-middle attacks and organization impersonation.





Jan, 2024

Mercedes Source Code Exposed by Leaked GitHub Token

A leaked token provided unrestricted access to the entire source code on Mercedes-Benz's GitHub Enterprise server.





Feb, 2024

***Infosys Discloses 57,000 Bank Of America
Customers Impacted By 2023 Breach***





Put it all
together

Jan, 2024

Mother of all breaches' data leak reveals 26 billion account records stolen from Twitter, LinkedIn, more





There is a cyber attack every

39 seconds.

NOW YOU

KNOW.

Common Attack Vectors Exploited



**Let's Secure-By-
Design**

BUT...

There's deadlines to meet.

Customers to please.

Not enough budget.

No buy-in.

Don't have the skills.

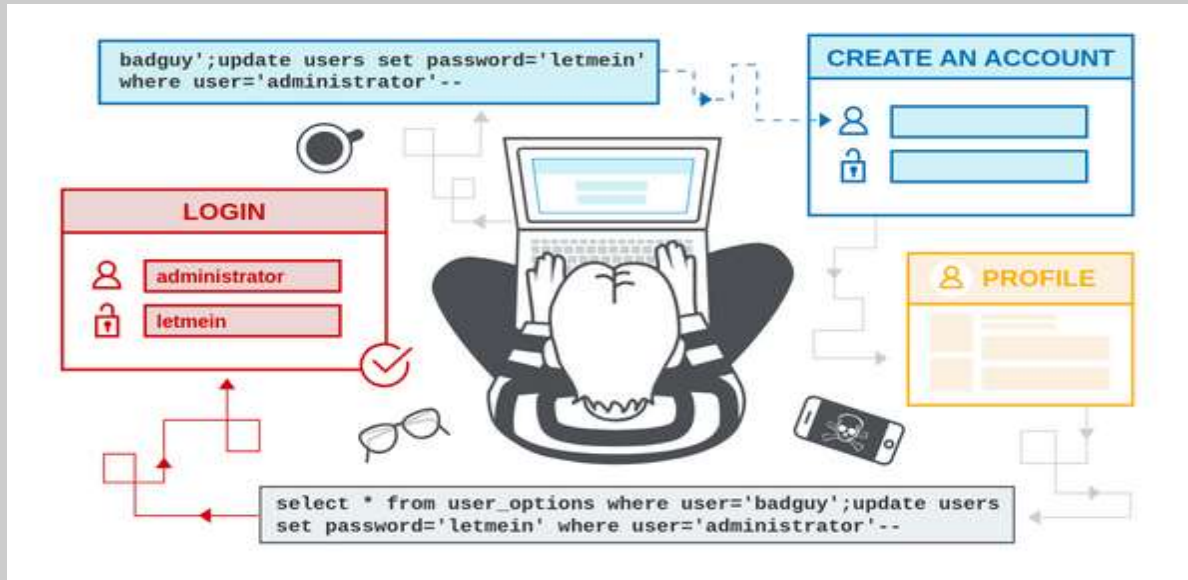
We'll just do it when there's a breach!

We're not big enough.

Is it really that hard to start thinking about security from the start?



SQL Injection



Input Validation

Use Parameterized Queries

Whitelisting Allowed Values

Indirect Object Reference - IDOR

```
https://insecure-  
website.com/customer_account?customer_number=1  
32355
```

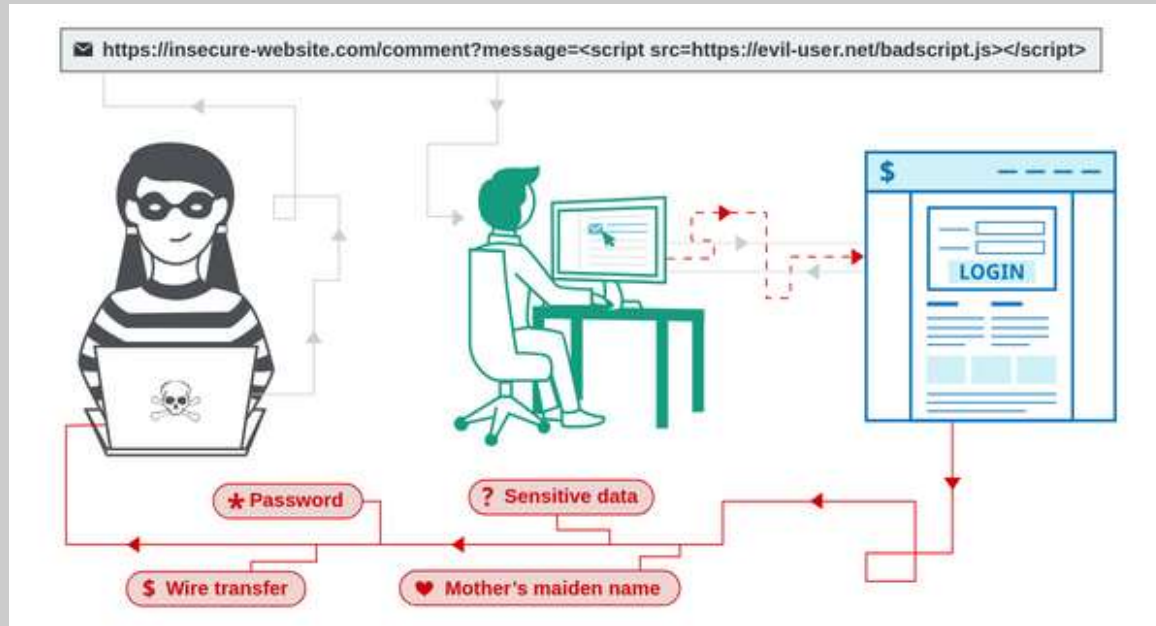
```
https://insecure-website.com/static/12144.txt
```

Input Validation

**Avoid direct object
references**

Implement GUIDs

Cross Site Scripting - XSS



Input Validation

Encode Data on Output

Use HTTP Headers

Default Credentials In Devices/Services

PostgresDB **'postgres'**

Wordpress - **'admin'**

Routers **'admin/admin'**

MySQLDB - **'root'**

Force Username Change

Add Strong Passwords

Enforce Policies

API Access Control

```
GET /api/v1/profiles/{userId}
```

```
POST /api/v1/transactions/sendMoney
```

```
{  
  "fromAccountId": "123",  
  "toAccountId": "456",  
  "amount": 1000.00  
}
```

Deny by Default

**Control Access with
JWT/OAuth/API Tokens**

**Add Rate Limiting to
Prevent DDoS**

Stack Traces

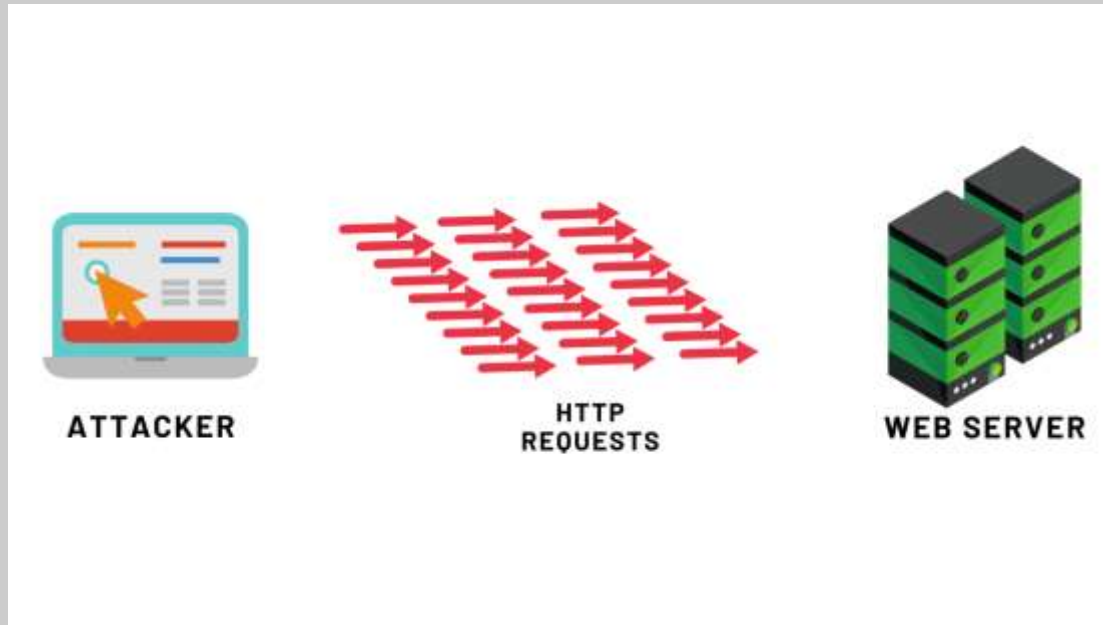
```
java.sql.SQLException: Access denied for user 'appUser'@'10.100.10.20' (using
password: YES)
    at com.mysql.jdbc.SQLException.createSQLException(SQLException.java:1075)
    at com.mysql.jdbc.MySQLIO.checkErrorPacket(MySQLIO.java:4096)
    at com.mysql.jdbc.ConnectionImpl.<init>(ConnectionImpl.java:794)
    at com.mysql.jdbc.JDBC4Connection.<init>(JDBC4Connection.java:47)
Caused by: java.sql.SQLException: Unable to connect to database.
    at application.database.ConnectionManager.getConnection(ConnectionManager.java:23)
    at application.user.UserDAO.getUserDetails(UserDAO.java:58)
User Details Query Failed: SELECT * FROM users WHERE user_id = ?
```

Log, Don't Display

**Use Error Handling
Frameworks**

Custom Error Pages

Rate Limiting



Captcha + OTP

Account Locking

API Limiting

Sensitive Data

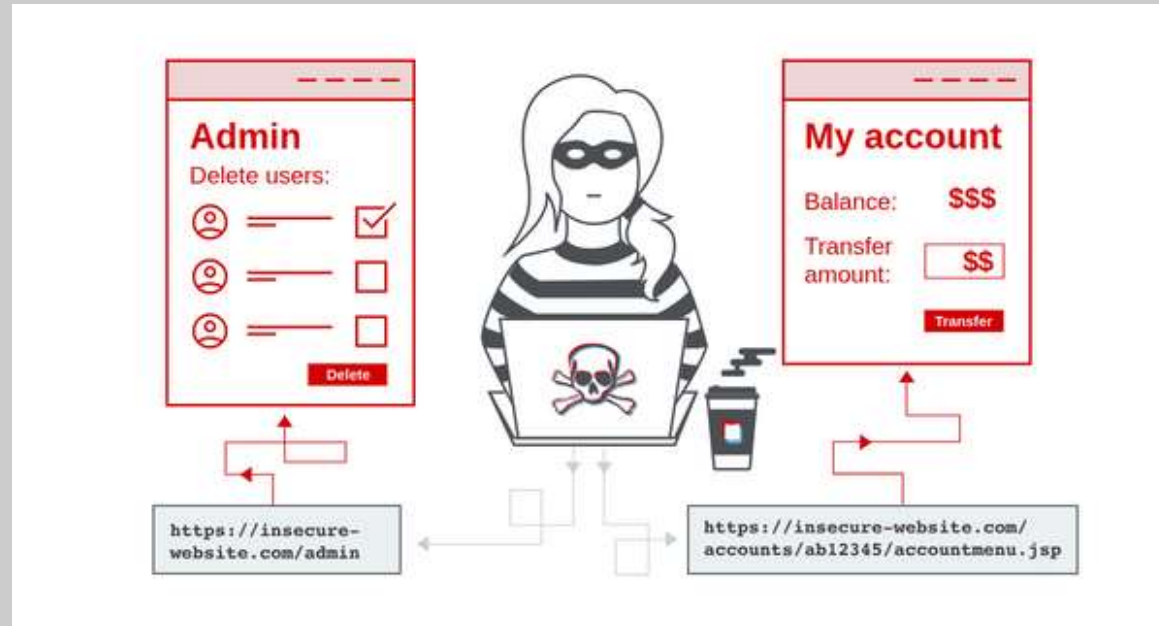
ID	Name	Date of Birth	PAN Card	Account Number	Bank Name	IFSC Code
1	John Doe	1985-07-24	ABCD1234E	123456789012	Bank A	IFSC000123A
2	Jane Smith	1990-05-16	EFGH5678F	987654321098	Bank B	IFSC000456B

Encrypt sensitive data

Enforce Access Controls

Perform Regular Data Audits

Access Control

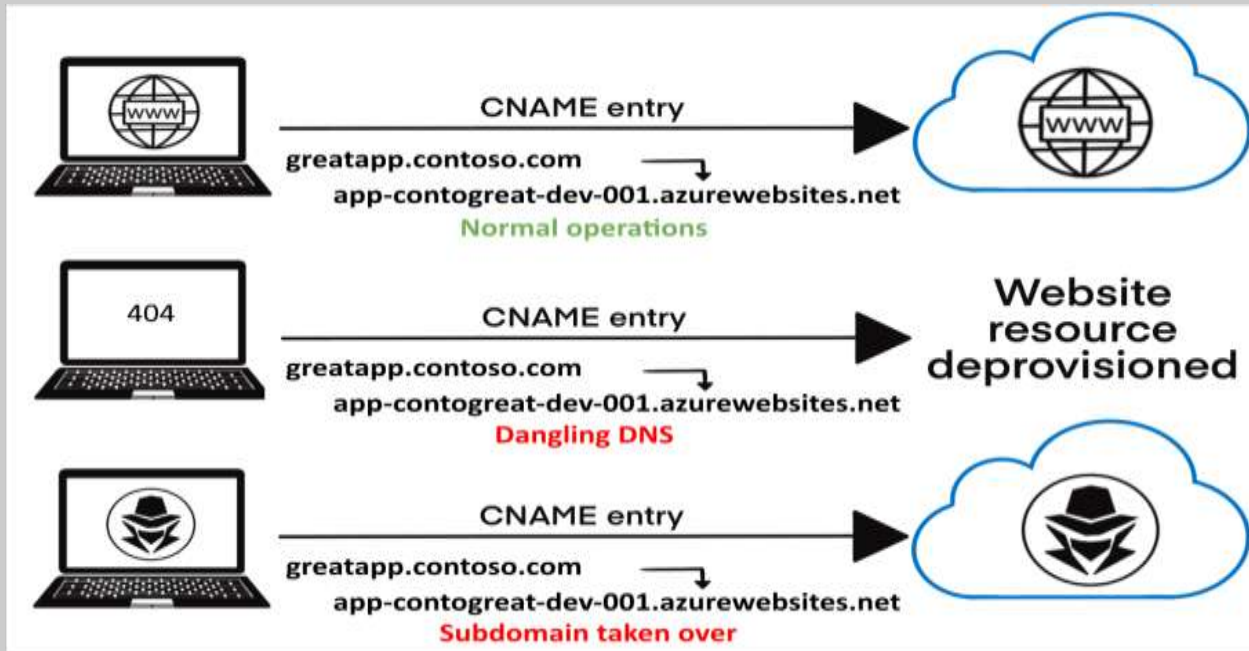


Deny by Default

**Create Single Access
Control Method**

Perform Regular Audits

Dangling SubDomains



Subdomain Inventory

Good DNS Habits

Regular Audits

Stronger Passwords

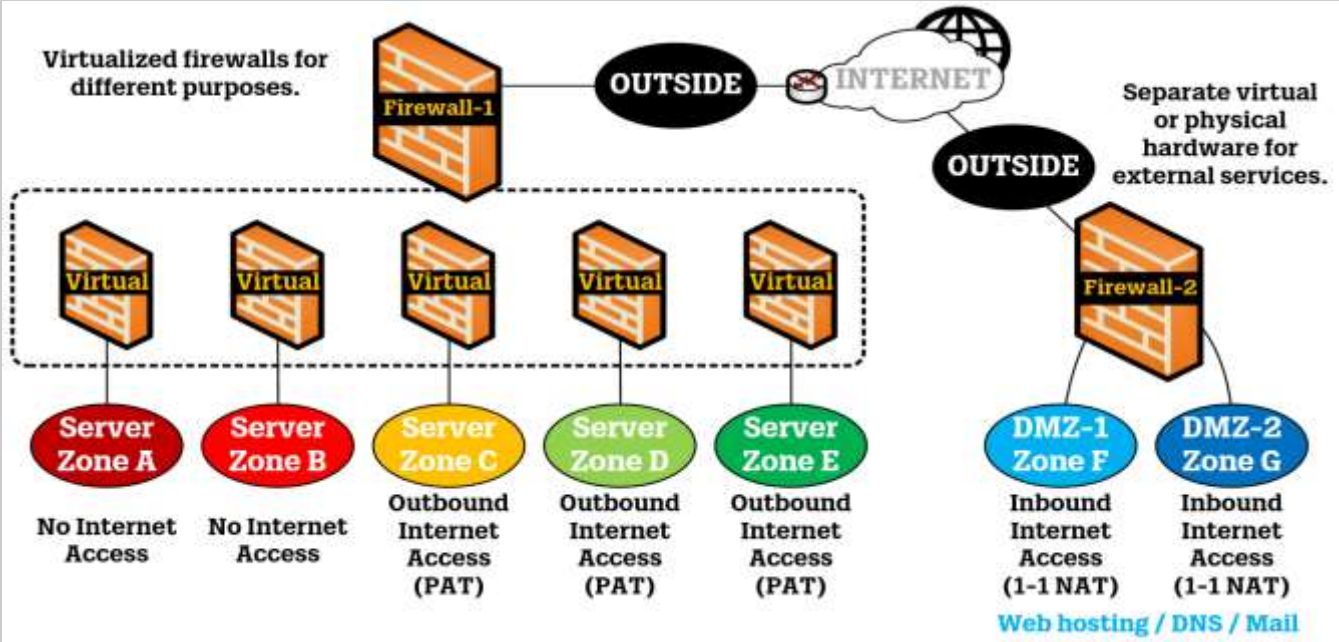
RANK ↕	PASSWORD ↕	TIME TAKEN TO CRACK ↕	NUMBER OF TIMES USED ↕
1	123456	< 1 Second	4,524,867
2	admin	< 1 Second	4,008,850
3	12345678	< 1 Second	1,371,152
4	123456789	< 1 Second	1,213,047
5	1234	< 1 Second	969,811
6	12345	< 1 Second	728,414
7	password	< 1 Second	710,321
8	123	< 1 Second	528,086
9	Aa123456	< 1 Second	319,725
10	1234567890	< 1 Second	302,709

Make Them Complex

Use a Longer Password

Opt for MFA

Network Segmentation



Isolate Critical Systems

Control Access

Monitor Traffic

Logging

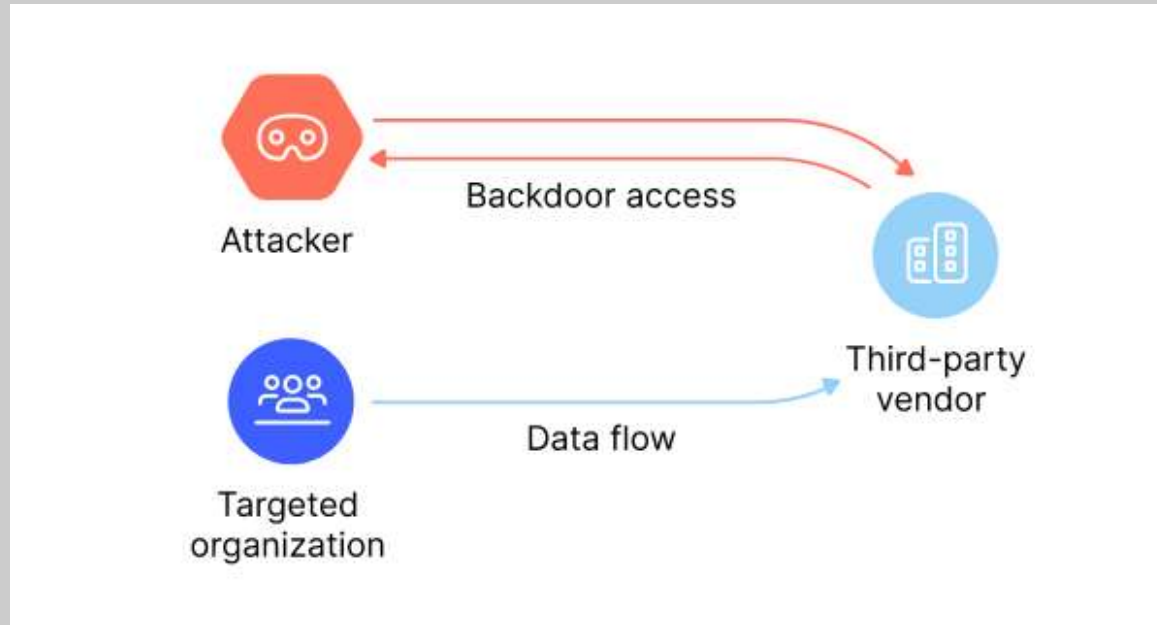
```
Jun 24 13:45:34 httpd: [2024-06-24 13:45:34] 1x-ewe-ws2-02.ix.netcom.com [30:01:46:46] GET /EPA-WASTE/1994/October/Day-05/ HTTP/1.0" 200 598
Jun 24 13:45:36 httpd: [2024-06-24 13:45:36] dd14-034.compuserve.com [30:01:46:58] GET /logos/small_logoar.gif HTTP/1.0" 200 935
Jun 24 13:45:38 httpd: [2024-06-24 13:45:38] dd14-034.compuserve.com [30:01:46:58] GET /logos/small_fig.gif HTTP/1.0" 200 124
Jun 24 13:45:40 httpd: [2024-06-24 13:45:40] 1x-ewe-ws2-02.ix.netcom.com [30:01:46:55] GET /docs/EPA-WASTE/1994/October/Day-05 HTTP/1.0" 302 -
Jun 24 13:45:40 httpd: [2024-06-24 13:45:40] dd14-034.compuserve.com [30:01:46:58] GET /icons/book.gif HTTP/1.0" 200 156
Jun 24 13:45:41 httpd: [2024-06-24 13:45:41] 1x-ewe-ws2-02.ix.netcom.com [30:01:46:56] GET /EPA-WASTE/1994/October/Day-05/ HTTP/1.0" 200 623
Jun 24 13:45:42 httpd: [2024-06-24 13:45:42] dd14-034.compuserve.com [30:01:46:58] GET /logos/us_flag.gif HTTP/1.0" 200 2789
Jun 24 13:45:43 httpd: [2024-06-24 13:45:43] 1x-ewe-ws2-02.ix.netcom.com [30:01:47:12] GET /docs/EPA-WASTE/1994/October/Day-03 HTTP/1.0" 302 -
Jun 24 13:45:45 httpd: [2024-06-24 13:45:45] 1x-ewe-ws2-02.ix.netcom.com [30:01:47:14] GET /EPA-WASTE/1994/October/Day-03/ HTTP/1.0" 200 785
Jun 24 13:45:46 httpd: [2024-06-24 13:45:46] dd14-034.compuserve.com [30:01:47:19] GET /icons/ok2-0.gif HTTP/1.0" 200 231
Jun 24 13:45:48 httpd: [2024-06-24 13:45:48] bettang_client.uq.or.au [30:01:47:24] GET /enviro/html/emcl/emcl-overview.html HTTP/1.0" 200 2352
Jun 24 13:45:49 httpd: [2024-06-24 13:45:49] bettang_client.uq.or.au [30:01:47:31] GET /enviro/gif/wfacts.gif HTTP/1.0" 200 1367
Jun 24 13:45:50 httpd: [2024-06-24 13:45:50] 202.96.29.111 [30:01:47:34] GET /press/releases/ HTTP/1.0" 200 1243
Jun 24 13:45:51 httpd: [2024-06-24 13:45:51] bettang_client.uq.or.au [30:01:47:37] GET /enviro/gif/blueball.gif HTTP/1.0" 200 503
Jun 24 13:45:53 httpd: [2024-06-24 13:45:53] 1x-ewe-ws2-02.ix.netcom.com [30:01:47:37] GET /Rules.html HTTP/1.0" 200 3273
Jun 24 13:45:53 httpd: [2024-06-24 13:45:53] 202.96.29.111 [30:01:47:58] GET /icons/circle_logo_small.gif HTTP/1.0" 200 2624
Jun 24 13:45:54 httpd: [2024-06-24 13:45:54] 202.96.29.111 [30:01:48:04] POST /cgi-bin/htmlspite?334.67.99.11&url=http://www.gow218-20097.com/html/index/pressrel/index.php?R4&start=0.00&if=es HTTP/1.0" 200 3993
Jun 24 13:45:54 httpd: [2024-06-24 13:45:54] 202.96.29.111 [30:01:48:16] GET /advertisers/text.shtm HTTP/1.0" 200 527
Jun 24 13:45:55 httpd: [2024-06-24 13:45:55] dd14-034.compuserve.com [30:01:48:22] GET /Rules.html HTTP/1.0" 200 3273
Jun 24 13:45:57 httpd: [2024-06-24 13:45:57] www-c8.proxy.aol.com [30:01:48:23] GET /docs/searchable.html HTTP/1.0" 200 705
Jun 24 13:45:58 httpd: [2024-06-24 13:45:58] bettang_client.uq.or.au [30:01:48:25] GET /enviro/gif/banner.gif HTTP/1.0" 200 14887
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT "users" * FROM "users" WHERE "users"."id" = $1 ORDER BY "users"."id" ASC LIMIT 1 [ ["id", 1]]
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT COUNT(*) FROM "products"
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT COUNT(*) FROM "products"
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT COUNT(*) FROM "products"
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT "products" * FROM "products" ORDER BY products.updated_at desc LIMIT 1
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT "users" * FROM "users" ORDER BY users.updated_at desc LIMIT 1
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) SELECT COUNT(*) FROM "users"
Jun 24 13:54:14 httpd: [2024-06-24 13:54:14] User Load (1.76) method=GET path=/w/format.html controller=rolls_admin/main action=dashboard status=200 duration=35.71 view=20.85 db=6.39
remote_ip=23.252.53.179 user_id=1 params=[]
Jun 24 13:54:16 httpd: [2024-06-24 13:54:16] User Load (1.76) method=GET path=/at-info method=GET path=/a/product?_pjax=&S&data-pjax=container%5D host=form-trivia-72.herokuapp.com
request_id=407f806e-63bc-4830-8844-ec3eb0a780d7 web=23.252.53.179 dyno=web-1 connect=3m service=182ms status=200 bytes=17398
Jun 24 13:54:16 httpd: [2024-06-24 13:54:16] User Load (1.76) Product Load (1.76) SELECT "products" * FROM "products" ORDER BY products.id desc LIMIT 20 OFFSET 0
Jun 24 13:54:16 httpd: [2024-06-24 13:54:16] User Load (1.76) User Load (1.76) SELECT "users" * FROM "users" WHERE "users"."id" = $1 ORDER BY "users"."id" ASC LIMIT 1
[["id", 1]]
Jun 24 13:54:16 httpd: [2024-06-24 13:54:16] User Load (1.76) SELECT COUNT(*) FROM "products"
Jun 24 13:54:16 httpd: [2024-06-24 13:54:16] User Load (1.76) method=GET path=/w/product_format.html controller=full_admin/main action=index status=200 duration=76.99 view=64.78
db=18 remote_ip=23.252.53.179 user_id=1 params={"_pjax"=>"[data-pjax=container]", "model_name"=>"product"}
Jun 24 13:57:03 httpd: [2024-06-24 13:57:03] User Load (1.76) salt: Accepted publicly for samantha from 4.28.11.28 port 37884 sha2
Jun 24 13:57:03 httpd: [2024-06-24 13:57:03] User Load (1.76) salt: pam_unix(cash:session): session opened for user samantha by (uid=0)
```

Full Log Coverage

Troubleshooting

Tamperproof Logs

Supply Chain



Least Privilege Access

Network Segmentation

Identify Critical Asset

Too Much To Do. Start with these 5.

And - then just check regularly!

Authentication

Test authentication. Add MFA.

Validate Input

One bad input is all you need.

Access Control

Authorize. Deny by default.

Secure PII Data

Encrypt sensitive data. Isn't data what it's all about!

Secure Network

One misconfigured firewall, one extra port can be it.



Looking Ahead.

#1. AI Threats and Defense

#2. Spike in Third-Party Data Breaches

#3. Cyber Expertise in the Boardroom

#4. Identity and Access Management

#5. Nation-State Cyber Operations





STILL ON THE FENCE?



Perhaps, this will give you some joy.

<https://haveibeenpwned.com/>



Time to BUZZ?

REACH OUT!

