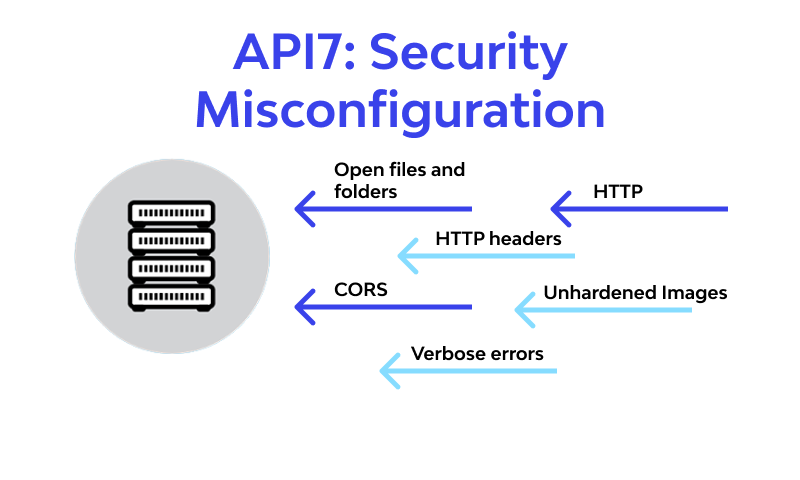
Security Misconfiguratin

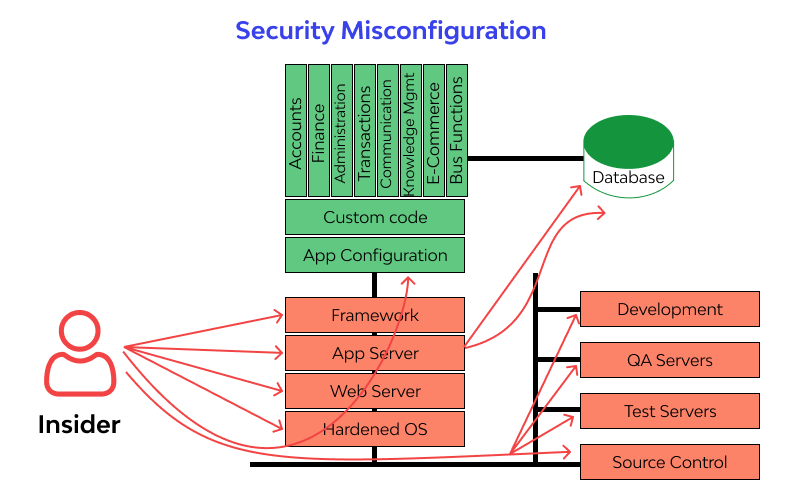


Introduction

When   security  settings  are  not   properly  defined   during  the  configuration   process   or  are   
maintained  and  deployed with  default settings,  security misconfiguration  happens.  Any layer  of   
the  application  stack, cloud,  or network could  be affected  by this.  Misconfigured  clouds are a   
major contributor to  data  breaches,  which  end  up  costing businesses  millions  of dollars.  In  most   
cases,    vulnerabilities    are   introduced    during    configuration.    Common    misconfiguration   
vulnerabilities  occurs  with  the  use of the defaults  which  includes passwords,  certificates and   
installation,  deprecated  protocols  and  encryption open  database instances,  directory listing which    
is  not  to  be enabled,  error messages  showing confidential  information,  misconfigured  cloud   
settings and  unnecessary features includi s including  pages,  ports a ports and c nd command inj nd injection.

Numerous  factors  can  lead  to  a misconfiguration. Due to  the  complexity and  constant  change of   
today's  network  infrastructures,  organizations  may overlook  crucial  security settings,  such  as   
those on ne those on ne those on network  equipment t nt that m t may  still  be  using  its def s default  settings.

You  must routinely audit security controls  and configurations  to  spot configuration  drift,  even  if   
an  organization  has  secured  configurations  for its  endpoints.  Misconfigurations  are made worse   
by  the  addition of ne ion of ne ion of new ha w hardware  to t  to the  network,  changing  systems, and ins stems, and ins stems, and installing  patches.



Network shares  and  firewall rules  may be created  by developers  for convenience while  software   
is  built keeping them  unaltered.  Administrators occasionally allow  configuration  changes  for   
testing  or tr  or troubleshooting, but t , but t , but these changes n s never put the c r put the c r put the c r put the configuration ba on back to i k to i k to its orig ts original st inal state.

If  an  antivirus pr virus prevents  certain a in actions (like r ons (like r ons (like running  installers),  employees  frequently  temporarily   
disable  it before forgetting to  re-enable  it.  More than  20%  of endpoints  are thought  to  be running    
out-of-date  antivirus or virus or  anti-malware  software.( D ( Dizdar a r and S nd Security, 2022) , 2022)

Impact  of  Security  Misconfigurations  Attacks

An  application  may be vulnerable  to  attack  as  a result of security misconfigurations,  which  can   
be the  result of relatively simple  errors.  A  cybercriminal  may not  even  need  to  launch  an  active   
attack  because  in  some  cases,  misconfiguration  may expose  data.  The risk  to  application  security   
increases as c s as c s as code  and da nd data  are  made  more  accessible to use le to use le to users.

For instance,  a database server  with  improper  configuration  may allow  data to  be accessed  via  a   
standard  web  search.  An attacker  might  be able  to  access  additional  data  outside of the  database   
or  launch a h another a r attack  on the c on the c on the company's ser 's servers  if this  if this  data c ta contains a ontains administrator c tor credentials.

Numerous  sensitive  and personal pieces  of information  may be made available  to  the public   
online due to  improperly configured (or non-existent)  security controls  on  storage devices.  In    
most cases,  it is  impossible  to  determine who  might  have had  access  to  this  information  prior  to   
its sec s security.

Another  frequent  problem   with   web   applications,  particularly those built  using pre-existing   
frameworks  like WordPress,  is  directory listing. Users  are free to  browse and  access  the file   
structure, makin , making  it  simple f ple for  them to find a  them to find a  them to find a  them to find and ta nd take  advantage  of se  of security flaws.

Attackers  can  use an  application's  structure to  modify specific  parts  of it or  reverse-engineer  it if    
you  can't  prevent  access  to  it.  If  an  application  is  designed to  be delivered to  mobile  devices,  it   
might  be difficult  to  manage this.  Using mobile  applications  weakens  an  organization's  ability to   
control  who  can  view or edit the  code,  as  noted  by OWASP.  This  is  due to  the  fact  that  a mobile   
device,  not  a proprietary server,  is  used to  deploy the business  and  presentation  layers of the   
applications.  (Dizdar a r and  Security, 2022 , 2022)

5  Common  Types  of  Security Misconfiguration

Common  events  in  an  IT environment  that  could  result in  a security misconfiguration  include the   
following:

    Default passwords  and  accounts are activated— It  is  a common  security mistake to  use

vendor-supplied  defaults  for system  accounts and passwords,  which  could give  attackers   
access t ss to the s o the s o the system wit stem without author out authorization.

     Secure password  policy is  not  implemented  —Failure to  implement  a secure password    
 policy could  give  hackers  access  to  the system  without  authorization.  For example,  they   
 could  use  lists of popular  usernames  and  passwords  to  brute  force a username  and/or

password fie d field unt ld until  a  successful a ssful authentication.

    Incompatible software with  unpatched bugs  — When  software patches  are not  updated  as

part  of the software management  process,  attackers  may be able  to  inject  malicious  code   
that the a that the a that the application then  on then  executes.

    Unprotected files  and  directories—If attackers are able to  access restricted files  or parts    
 of the  server  directory using forceful  browsing or  other methods,  it may be possible  for

attackers to  rs to  exploit unpro t unprotected f ted files and s and  directories.

    Unused   features   are  enabled   or  installed—  If  these  elements   are  not  removed,   the

application  is  vulnerable to  misconfiguration  flaws  and may be exploited  by attackers   
using techniques  like code injection  to  insert  malicious  code that  the  application  then    
executes.

Security Misco rity Misconfiguration  Examples

    Amazon  S3: Many businesses  have suffered  data  breaches  as  a result of unprotected

storage buckets  on  Amazon's  well-known  S3  storage service.  For  instance,  the  US  Army   
Intelligence and  Security Command  unintentionally stored  sensitive  database files in  S3    
without  the pr  the proper a r authentication, som on, some  of w  of which  were  marked top s d top s d top secret.

    Mirai  **(**未来**):**The Mirai  was  a mega scale  botnet  which  infected network  devices  like

CCTV  cameras,  DVD   players,  and  home   routers  on   a large scale.  The botnet  took   
advantage   of   these   devices'   default   passwords,    which   were   insecure,   as   a   
misconfiguration.   Websites   like  Twitter,   Reddit,   and   Netflix  were  brought   down   by   
DDoS  attacks of unpr ks of unpr ks of unprecedented siz nted size, whic , which we h were carried out b d out b d out by  the  botnet.

    Attack    using   a   misconfigured    NASA    authorization:    NASA    is    susceptible    to    a

misconfiguration  in  Atlassian  JIRA.  Sensitive  data  was  exposed to  attackers  due to  an    
authorization mi on misconfiguration in Global P on in Global P on in Global P on in Global Permissions.

Safeguarding  Against Secu st Security Misco rity Misconfiguration

Safeguarding against a certain  security misconfiguration  involves  some major implementory

methods.  Creating a repeatable hardening process  to  make it quick  and  easy to  deploy new

environments  that  are correctly configured.  The configuration  of the  production,  development,    
and  QA  environments   must  be uniform,   but   each  environment   must  use  a different   set   of   
passwords. Autom ds. Automating  this proc his procedure  to  create a te a secure environment qui t quickly.

In  every environment,  installing software patches  and  updates  on  a regular and  timely basis.    
Additionally,   patching  of  a  golden   image  and  using  it  in   one’s   environment   can   be  done.   
Creating  an  application  architecture that  provides efficient  and  secure element  separation  is  also    
a  tremendous w mendous way  for  security  safeguarding.

Running  scans   and  audits   frequently  and   on  a  regular   basis  to   look   for  potential   security   
vulnerabilities  or missing patches.  Making  sure the  development  cycle  is  organized  and  well-   
maintained.  This  will make it easier to  test  the application's  security during the development   
stage.  Using  a  platform  with   the   bare  minimum   of  features,   documentation,   samples,   and   
components. Avoid i omponents. Avoid i omponents. Avoid installing  or r  or removing  unsafe frameworks or rks or  unused  features.

Examining the  permissions  for S3  buckets  and  other  cloud  storage.  Include patch  management   
updates  and  reviews  of all security configurations  for all updates,  security patches,  and  notes.    
(Poptani and G ni and G ni and Gatty, 2018 , 2018)

Conclusion

The most important  recommendations  are to  arrange most of the  accompanying a consistent

solidification  procedure that  makes  it quick  and  easy to  send  another  condition  that  is properly

secured.  Conditions  for QA,  generation,  and  improvement  should  all be created  similarly (with

various  passwords  utilized  as  a part  of every condition).  To  reduce the  effort  needed to  create  a

new  safe environment,  this  process  should  be computerized.   A  method  for keeping abreast  of

and  communicating all fresh  software updates  and  fixes  in a favorable manner  to  each  sent

condition. Addit ion. Additionally, t , this m his must i ust include a lude all  code libraries. A st s. A st s. A strong  application e on engineering that  ring that

provides   segmentation   that   is   compelling  and   secure.   To   aid   in   identifying  upcoming

configuration  errors  or  missing patches, think  about  periodically running sweeps  and performing

reviews.(Poptani and  ni and  Gatty, 2018) , 2018)

References

   Poptani, R optani, R. a . and Ga nd Gatty, P , P.,  2018. *Security  Misconfiguration*. [ . [online] Ijrp.org. Av . Available a ble at:

[<https://www.ijrp.org/paper-detail/265> [ /265> [Accessed 19 Oc d 19 Oc d 19 October 2022].](https://www.ijrp.org/paper-detail/265%3e)

   Dizdar,  A.  and  Security,  B.,  2022. *Security Misconfiguration:  Impact,  Examples,  and*

*Prevention*[.  [online] Bright  Security. Available at: <https://brightsec.com/blog/security-](https://brightsec.com/blog/security-)

misconfiguration/> [ on/> [Accessed 19 O ssed 19 O ssed 19 October 202 r 2022].

   Dizdar,  A.  and  Security,  B.,  2022. *Security Misconfiguration:  Impact,  Examples,  and*

*Prevention*[.  [online] Bright  Security. Available at: <https://brightsec.com/blog/security-](https://brightsec.com/blog/security-)

misconfiguration/> [ on/> [Accessed 19 O ssed 19 O ssed 19 October 202 r 2022].

   Poptani, R optani, R. a . and Ga nd Gatty, P , P.,  2018. *Security  Misconfiguration*. [ . [online] Ijrp.org. Av . Available a ble at:

[<https://www.ijrp.org/paper-detail/265> [ /265> [Accessed 19 Oc d 19 Oc d 19 October  2022].](https://www.ijrp.org/paper-detail/265%3e)