

# 聊一聊办公网安全建设

◆  
网易 / 沈明星



# 目录

办公网安全挑战

1

办公网安全建设框架

2

3

企业级实践经验

4

Q & A



# 挑战

## 人

人员复杂（实习、外包），流动性大，安全意识参差不齐

## 系统复杂

自研、采购、外包

## 企业文化

互联网企业相对比较宽松，员工反弹大



## 移动办公

家里、出差，办公室网络任意切

## 攻击面

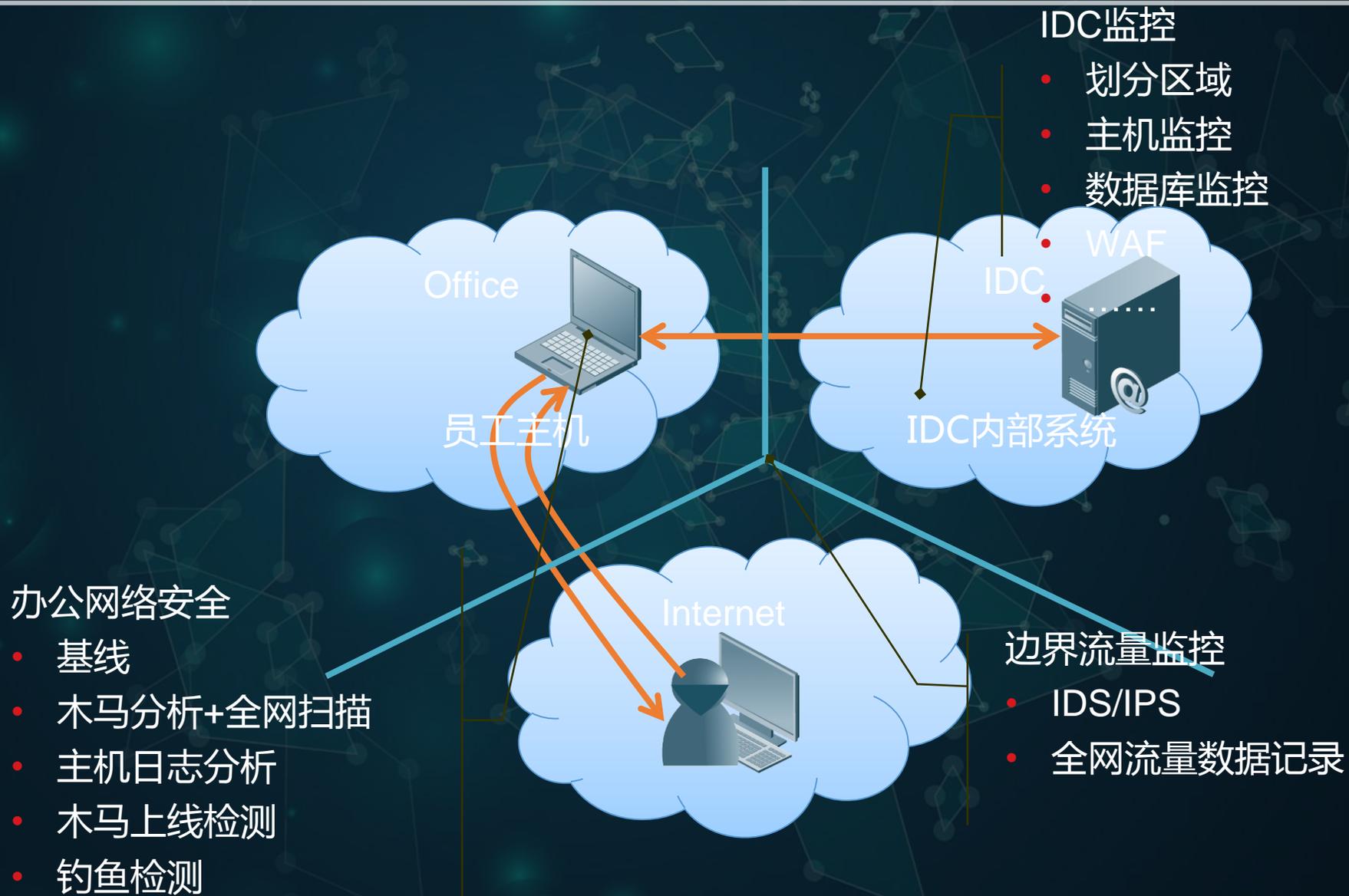
网络，系统，人，环境

## 多部门合作

IT、安全、HR、行政等



# 办公网边界



# 办公网络安全范围

- 有线网络 & 无线网络
- 办公区个人PC（台式机+笔记本）
- 自带笔记本等BYOD设备（手机，Pad，笔记本）
- 办公区服务器
- OA、HR、财务等内网系统
- 摄像头、门禁、车辆管理等系统
- 人和相关ID（正式员工，外包，实习生）



# 认证与授权

- 首先需要HR统一人员管理和ID
- 统一AD、邮箱账号和工号体系
- 统一3A
  - 统一认证处理
  - 统一授权管理
  - 统一进行审计





# 统一权限管理系统

统一权限管理平台 注销

系统管理

关键词搜索

系统名称	系统地址	更新时间	状态	责任人	操作
评测系统	http://[redacted].com	2018-07-01	已停用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
运维平台	http://[redacted].com	2018-06-27	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
管理系统 (前台)	http://[redacted].com	2018-06-21	已停用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">启用</a>
可视化系统	http://[redacted].com	2018-06-21	已停用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">启用</a>
图系统	http://[redacted].com	2018-06-21	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
预警系统	http://[redacted].com	2018-06-21	已停用	[redacted] se.com	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
踪系统	http://[redacted].com	2018-05-31	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
理系统	http://[redacted].com	2018-05-31	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
理系统	http://[redacted].com	2018-05-09	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
平台	http://[redacted].com	2018-05-07	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
后台管理平台	http://[redacted].com	2018-04-18	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
系统	http://[redacted].com	2018-04-16	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>
各管理平台	http://[redacted].com	2018-04-12	已启用	[redacted]	<a href="#">编辑</a> <a href="#">查看</a> <a href="#">查看关联用户</a> <a href="#">停用</a>

[用户操作手册](#)



# 网络准入

- VPN接入

- 逐步废掉私自搭建的OpenVPN通道
- 内部网站没有特殊情况，不对外开放

- 设备准入

- NAC
- Agent 支持身份认证和安全基线检测等功能
- 支持的终端类型和OS



# 终端安全

- 域控有点弱
- AV
- 补丁管理
- 软件管理



# WIFI 安全

---

- 私搭WIFI
- WIFI guest认证
- WIFI 钓鱼



# 网络隔离

- 服务器区
- 员工电脑区（根据职能适当划分）
- GUEST隔离
- 特殊岗位隔离，虚拟桌面（例如，审核）



# 网络安全

- 漏洞扫描
  - 服务器扫描
  - 主机扫描
- 安全设备
  - 防火墙
  - IDS / IPS / APT 与 终端安全AV等联动
- 对外开放服务端需要审核和备案



# 员工行为管理 & 数据安全

NDLP & HDLP

上网行为管理系统

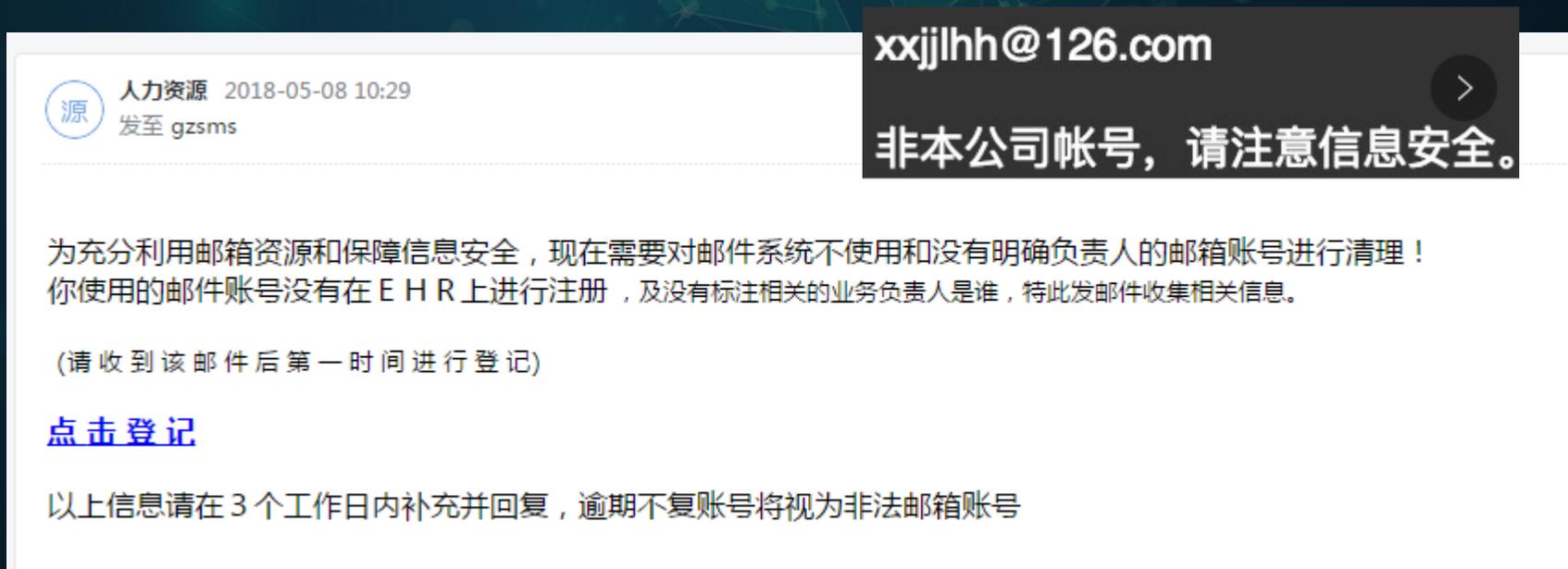
邮箱审计

水印（web水印、文件水印，桌面水印）



# 邮件安全

- 钓鱼邮件处置
- 邮件反垃圾



源 人力资源 2018-05-08 10:29  
发至 gzsms

xxjllhh@126.com  
非本公司帐号，请注意信息安全。

为充分利用邮箱资源和保障信息安全，现在需要对邮件系统不使用和没有明确负责人的邮箱账号进行清理！  
你使用的邮件账号没有在 E H R 上进行注册，及没有标注相关的业务负责人是谁，特此发邮件收集相关信息。

(请收到该邮件后第一时间进行登记)

[点击登记](#)

以上信息请在 3 个工作日内补充并回复，逾期不复账号将视为非法邮箱账号



# 第三方供应商安全 & 资产

- 三方设备维护制度
  - 跳板机 + 录屏软件 + 人肉监控
  - TeamViewer
  - Zoom
  - QQ远程
  - PCAnywhere
- 设备重复利用 & 硬盘清理



# 安全管理与运营

- 安全管理制度与流程文档（最佳实践梳理）
- 安全合规（符合法律法规与政府监管）
- 安全运营与定期巡检
  - 安全方案的实施与反馈、优化
  - 安全问题/风险的发现能力
  - 安全问题/事件根因分析



# 实践案例

4266835	2018-04-26 14:04:37	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	87.05 KB
4266831	2018-04-26 14:04:37	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	472.09 KB
4266827	2018-04-26 14:04:36	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	316.6 KB
4266823	2018-04-26 14:04:36	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	2.43 MB
4266819	2018-04-26 14:04:36	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	1.87 MB
4266815	2018-04-26 14:04:36	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	2.58 MB
4266811	2018-04-26 14:04:36	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	1.36 MB
4266807	2018-04-26 14:04:35	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	2.67 MB
4266803	2018-04-26 14:04:35	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	1.97 MB
4266799	2018-04-26 14:04:35	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	3.68 MB
4266795	2018-04-26 14:04:35	[Redacted]	HR部门	Endpoint removabl...	Seagate BUP GD	Medium	Permitted	1	1.99 MB

Incident: 4266819 Severity: Medium Action: Permitted Channel: Endpoint removable media

Display: Violation triggers

Rule: 文档检查策略

- Various Graphics Formats (File Type)
- E:\新正式员工档案
- 公司\_HR\_关键字 (Dictionary)
- 入职

Forensics Properties History

Source: [Redacted] Event Time: 26 Apr. 2018, 2:04:36 PM

Destination: Seagate BUP GD 移动硬盘

Details: File "E:\新正式员工档案" was copied to removable device

Additional forensics data is not available. Either the action plan for this rule does not include forensics; you do not have permission to view forensics; or the system was unable to retrieve f



# 实践案例

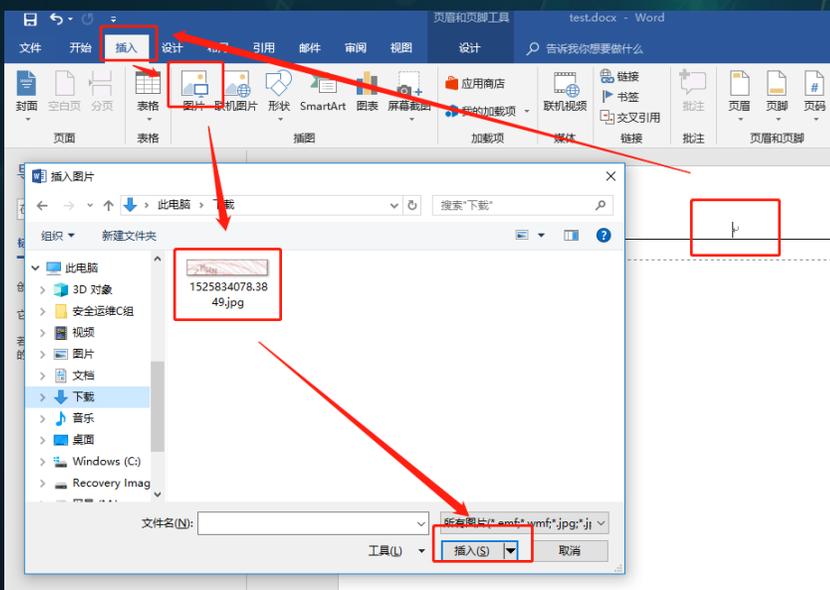
- 密码管理
  - 定期爆破和社工库比对密码
  - 通过1password对所有工作中用到的密码进行管理，全部使用自动生成的复杂密码，禁止使用个人常用密码，包括邮箱账号、域账号、内部系统账号、ssh key密钥、git key密钥等；



# 实践案例

atestexcel文档.xlsx - ZIP 压缩文件, 解包大小为 49,567 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
.._rels			文件夹		
docProps			文件夹		
NWM_h123_2018-07-12_17-22-49			文件夹	2018/7/12 17...	
NWM_H6666_2018-07-12_17-31-03			文件夹	2018/7/12 17...	
NWM_H8099_2018-07-12_17-14-53			文件夹	2018/7/12 17...	
NWM_H8099_2018-07-12_17-15-36			文件夹	2018/7/12 17...	
xl			文件夹		
[Content_Types].xml	1,556	377	XML 文档	1980/1/1 0:00	A458F7AA



# 实践案例

alertType	alerti	p	re	fileHash	sname	loca	malware_type	sev	occurred	mwurl	src	st	cnchost	channel
Malware Callback	193616	Web	wMPS (wMPS) 8.1.2		Trojan.Emotet	10 US/OH/North Olmsted		crit	2018-05-15T02:34:13Z	ht	10.240.116.40	bot-com	65.25.17.131	GET / HTTP/1.1 Cookie: 46815=LA9QWrmK5H4d1BnxXBWMftu/ZO mdyPCo2os4YCG5GgYNe6NAuNkEAqTRIEe 6qnhVq5Cm1ktqRxJP3Tj1pHvAzAqF1au nAMhj9RSZp/hXSYrIj6JRjeQbf9LR5d6GQV8 nPjvUAJXKbprMZ4Hb5yh0Gm1OIOqLJPDeg YLeYBlSqzyWNakdpp7iKU31kkOuvIvohaUb gN+kDQ/GPoX+t6crQ9aQtLt5O3Q6E4+IEh ANlivxKJ8LUW5QjydB3+nw87qWV9fSFENg OfPNUWPipQN7KpatX3yOW2vekkPpouizc mop2nNz8FZxYrdlWXGnn5xJaFmMGBn0FLi b0Xm+uqTOSvG76vHLV9uonp/MdMPkAS uziHQXW56RntYqqNea7wJ5FfleLB8eJfaZUD V/0tIrlJelCztHJVzehqUSwYvG7wQwhdUpzPic oN4dv5qXkQbbGV45LO8ymfknIERAokJJZfx ZaWRB4JzJ59pOfcOTSniG0jCYD+OebP0AGc bNNQeXx/VhLvoZRkiPuJdUyUX/LIFz0Fux0 mRjCQMvfVsDW7eXRTIBP6L0UvicrowKNSLR bk5xh3PI7BOythTa0kNIYHWTkGH58bkHR4q N11OndmVUjfmFx0E/yNK+ELjToI3zHXfbC5 P23mQzODsq4qxMDryct5Bx00MbWo5/rIHP MI9MpuLsa/u8PlrC35JF18zgQ== User- Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 65.25.17.131 Connection: Keep-Alive Cache- Control: no-cache





**THANKS**



2018 携程安全沙龙