远程办公的企业信息安全

熊思敏　UCloud高级安全工程师

UCLOUD优刻得

共抗疫情，守望相助

冠状病毒疫情牵动全国，影响到每个家庭。UCloud作为一家云计算企业，我们希望能在这个特殊的时刻，用我们的技术和资源，同大家一起，携手为抗击疫情贡献一些力量。

我们关注到很多伙伴企业以各种形式在帮助灾区，我们特此声明：

凡是与灾区疫情相关的紧急救助项目，不论是否是我们现有用户，只要有需求，我们将提供免费的云计算资源与技术支持，包括且不限于：云主机、带宽、CDN、RTC、存储等，以及远程IT方案咨询与服务支持。

这些紧急救助项目，包括且不限于：政务信息的及时同步，医疗信息同步、免费教育资源提供，在线医疗、物流、援助信息撮合、寻人系统等企业级用户，我们不仅将提供免费云计算资源，也会提供技术方案的支持帮助。

除此之外，UCloud也通过各种途径，在全球多个地方收集医疗物资，发送武汉和湖北其他地区。我们向坚强奉献的广大医护工作者致敬，向奋战在疫情一线的各行业工作人员致敬！相信在全国人民的守望相助下，这场抗击疫情攻坚战一定能够取得胜利！

服务热线：400-0188-113转2　　UCloud技术支持团队，7x24小时随时提供云服务支持

远程办公下面临的安全挑战

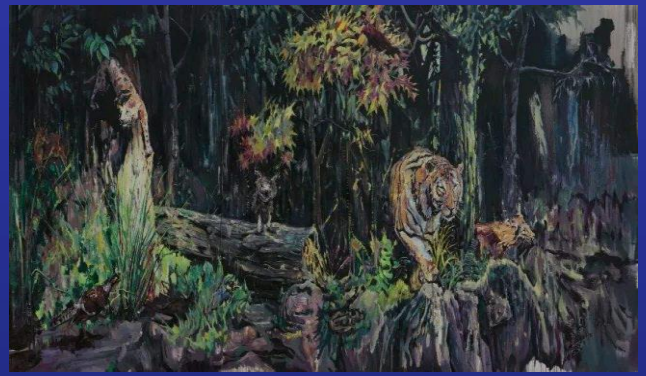
- 企业和个人从相对封闭安全的内网走出，面对风险满布的互联网

企业: 如何在对外开放满足员工远程办公需求的前提下确保自身信息资产的安全?

员工: 在开放的网络环境下如何抵御恶意攻击实现安全的远程办公?

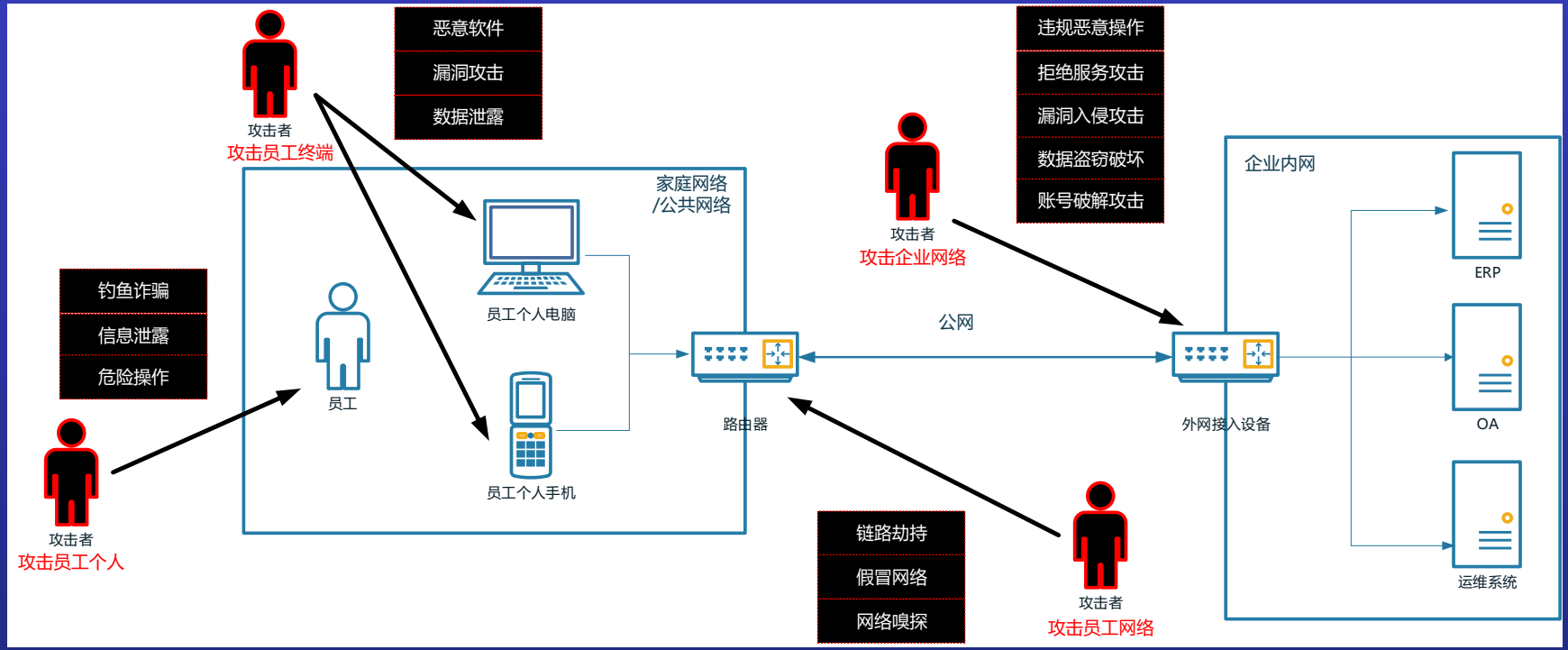
安全的温室

危险的丛林



远程办公下面临的信息安全风险

远程办公下员工和企业都会遭受比原有封闭内网更多的安全风险



企业后端系统安全

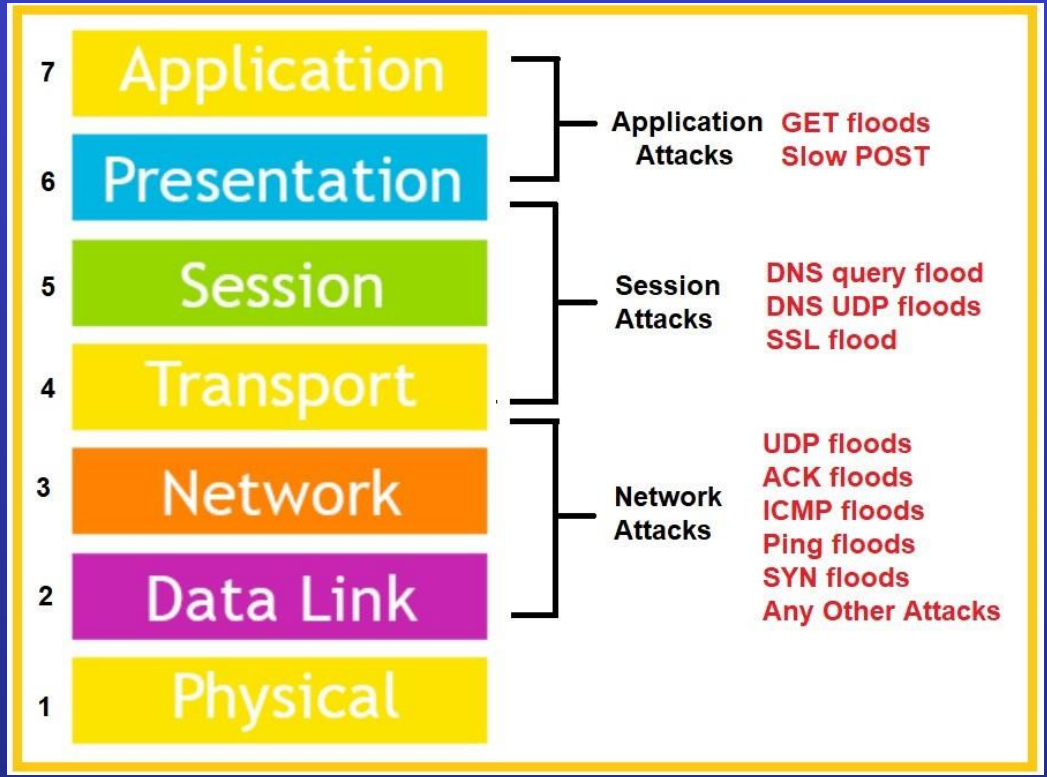
- 企业后端系统从内网走向互联网存在严峻安全考验

  - 没有经过严格安全测试
  - 鉴权强度不够(弱密码/暴力破解等)
  - 权限细分不够
  - 没有良好容灾
  - 软件补丁更新不及时
  - 缺乏监控和审计
  - 没有数据防泄密保护

企业后端系统安全

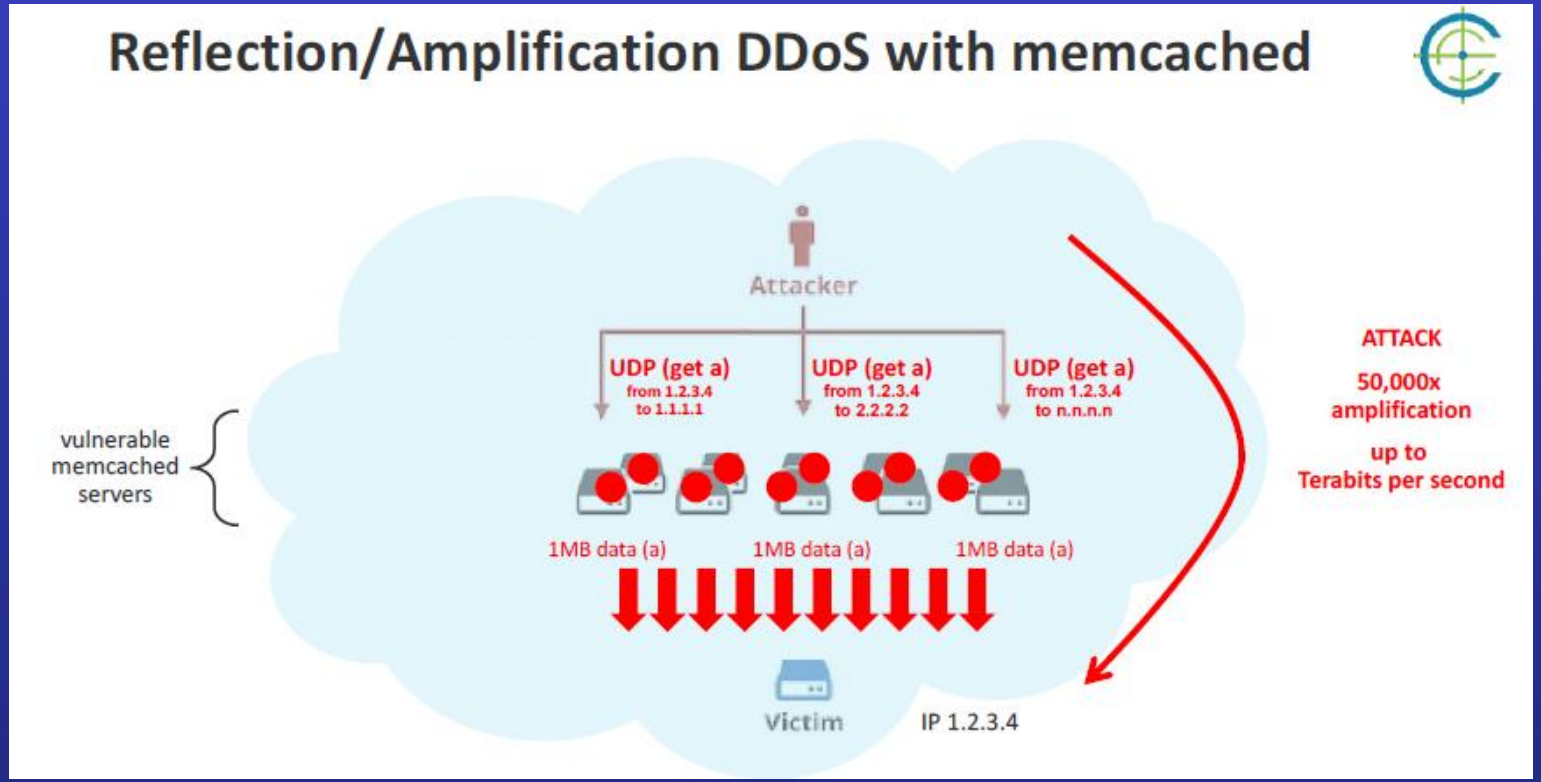
- 拒绝服务攻击

攻击者利用大量“肉鸡”对目标发动大量的正常或非正常请求、耗尽目标主机资源或网络资源，从而使被攻击的主机不能为合法用户提供服务。典型有ICMP Flood/UDP Flood/NTP Flood/SYN Flood/DNS Query Flood/CC攻击等



企业后端系统安全

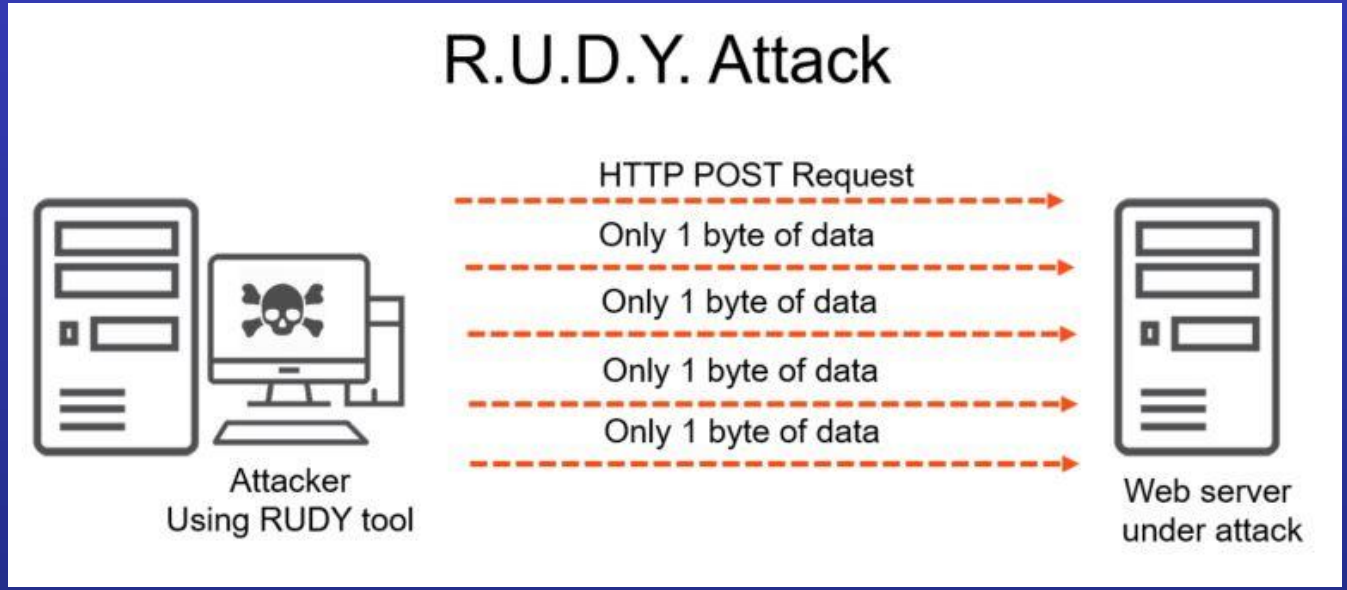
- 典型拒绝服务攻击 — memcached反射攻击



企业后端系统安全

- 典型拒绝服务攻击 — RUDY

  慢速HTTP POST请求方式进行DDOS攻击



企业后端系统安全

- 漏洞入侵攻击

入侵者通过企业开放在外网服务的漏洞进行入侵攻击，包括但不限于web框架、开源软件、商业软件等，主要是通过一些已经公开但是企业未能及时修复的漏洞。

美国征信巨头Equifax大规模数据泄露的惨痛教训：不及时修复漏洞，就是给自己埋不定时炸弹

AngelaY 2017-09-15 共502770人围观，发现 1 个不明物体 观点 资讯

美国征信巨头 Equifax 日前确认，黑客利用其系统中未修复的 Apache Struts 漏洞（ CVE-2017-5638，3 月 6 日曝光）发起攻击，导致了最近影响恶劣的大规模数据泄漏事件。Equifax 是美国三大老牌征信机构之一，拥有大量美国公民敏感数据，收益一直在 10 亿级别。其原本提供免费信用监控和身份窃取保护服务，还声称可以安全地冻结对敏感信息的访问。此次大规模数据泄露对其而言无疑是一场灾难。

美国征信巨头 Equifax 泄露了 1.45 亿用户数据，一人赔 125 美元

美国网络安全和基础设施安全局 (CISA) 于 1 月 10 日警告企业，修补其 Pulse Secure VPN 服务器以防止利用漏洞 CVE-2019-11510 的攻击。

该漏洞使未经身份验证的远程攻击者可以发送特制的 URI，以连接到易受攻击的服务器并读取包含用户凭据的敏感文件，并在后继的攻击阶段用于控制组织的系统等。

在未打补丁的系统上，该漏洞允许无有效用户名和密码的人远程连接到公司网络，关闭多因素身份验证控制，远程查看纯文本日志（包括 Active Directory 帐户和缓存的密码）。

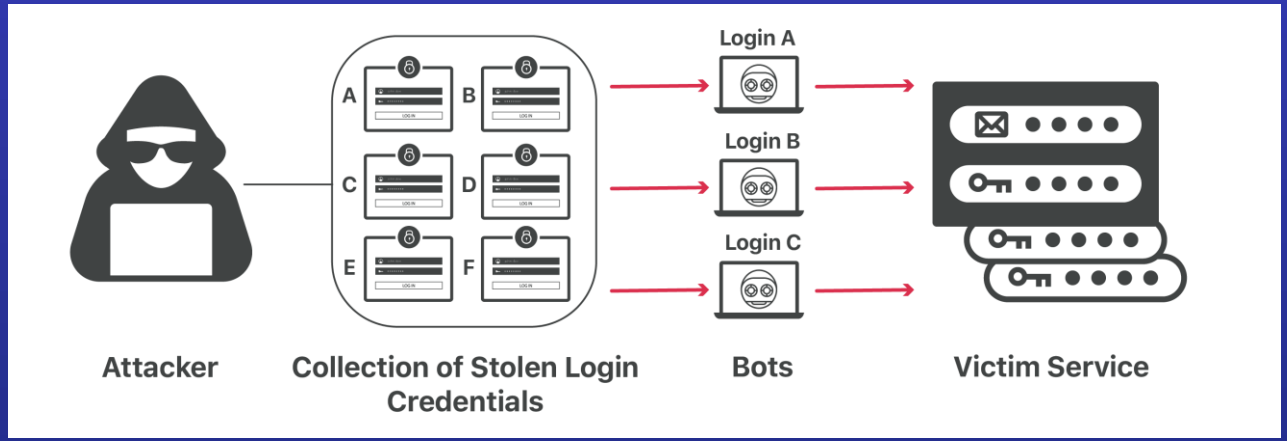
美国多家机构实体遭到入侵

FBI 表示，自 2019 年 8 月以来，身份不明的威胁行为者已使用 CVE-2019-11510 安全漏洞“入侵著名的美国实体机构”，包括一家金融机构和一个市政府网络。

企业后端系统安全

- 账号破解攻击

入侵者通过盗窃、穷举等方式通过外网破解登录账号，登录企业的办公系统进而进行攻击，常见攻击方式有撞库、暴力破解等。



企业后端系统安全

- 数据盗窃泄露

存储在企业内网的数据可能因为不安全的对外开放、系统漏洞等原因导致数据泄露

企业后端系统安全

- 违规恶意操作

员工或者攻击者利用企业系统漏洞进行恶意操作，譬如盗窃数据、植入木马等。

电子邮件提供商VFEmail表示，它遭遇了灾难性的破坏：一个不知名的攻击者破坏了它的所有服务器，短短几小时内彻底清除掉了近二十年来的数据和备份。

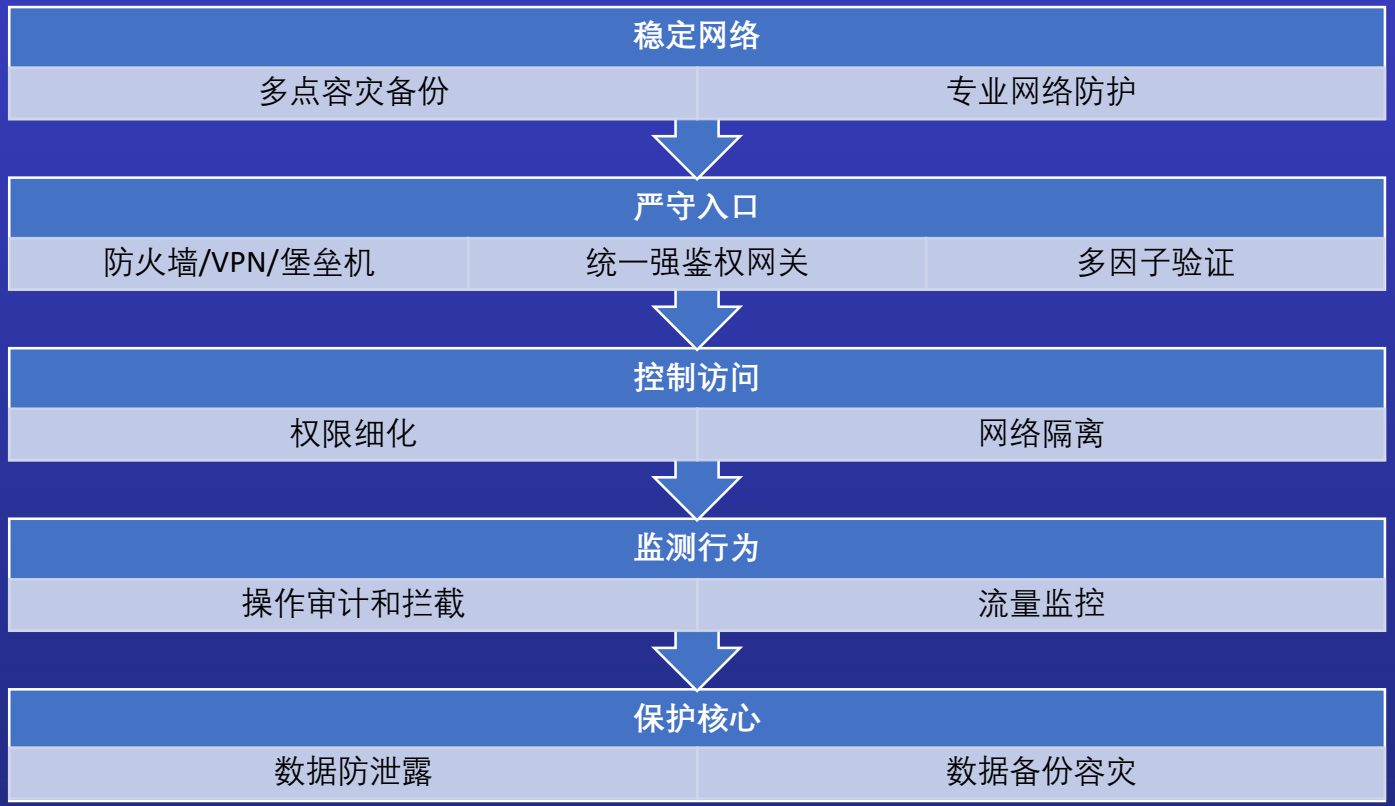
VFEmail创始人Rick Romero周二上午在Twitter上发推文道："是的，@VFEmail实际上销声匿迹了。"他看到有人对他在2001年创办的这项服务的硬盘有条不紊地进行格式化。"数据可能回不来了。我从未想过有人会如此关注我的劳动成果，以至于想要完全彻底销毁它。"

日前，中国裁判文书网公布这样一起案例，一名比特大陆员工远程入侵公司租用的阿里云服务器，盗窃100个比特币。

根据裁判文书，被告人仲某某自2015年11月16日起担任北京比特大陆科技有限公司（以下简称"比特大陆公司"）运维开发工程师。2017年9月15日18时许至次日1时许，其在北京市海淀区，通过使用TEAMVIEWER软件远程控制其在比特大陆公司工位上的电脑，使用ROOT权限进入公司租用的阿里云服务器，在比特币钱包程序中插入代码转移了比特币100个至其在互联网站的个人"钱包"里。同年9月16日9时许，比特大陆公司发现网络上公司的比特币余额不足，

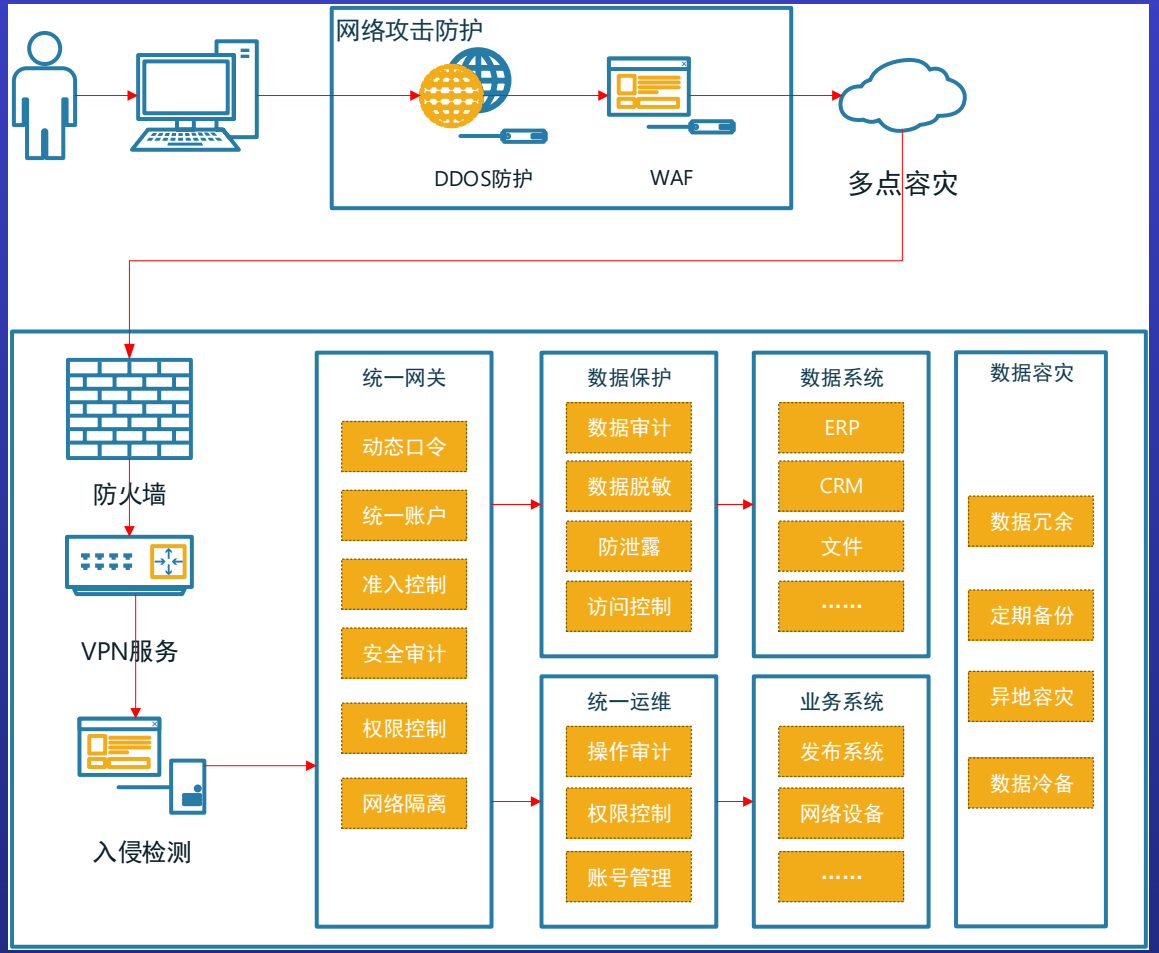
企业后端系统安全

层层设防确保稳定和安全



企业后端系统安全

- 层层设防立体化防护
- 网络多点容灾确保系统高可用
- 不要让内部系统直接对外暴露
- 通过VPN/防火墙控制网络准入
- 网络攻击防护必须前置
- 隐藏后端入口IP
- 统一强鉴权保护系统账户
- 审计操作和被读取的数据
- 数据备份容灾



企业后端系统安全

- 典型案例应对思路: 怎么应对员工误操作或者恶意导致的删库?

事前预防

- 权限分离和细化和定期梳理和回收权限
- 统一运维平台并拦截高危操作
- 对员工进行典型案例宣传

事中发现

- 危险操作审计和告警
- 系统健康度监控

事后容灾

- 多点进行冷备和热备
- 使用云厂商的云存储

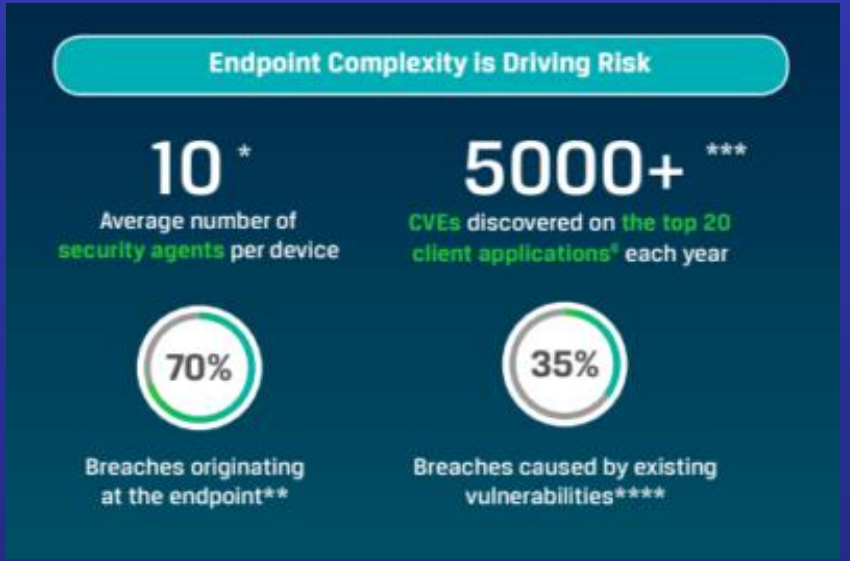
员工终端安全

- 远程办公的开放性对员工终端安全提出了严峻挑战

- 非标准化加固的终端
  (操作系统不一致/硬件不一致等)
- 如何识别合法终端拦截恶意终端
- 如何对所有终端进行安全漏洞修复
- 受病毒感染终端的及时隔离
- 员工所用软件的安全性
- 终端存储的数据安全

  .....

根据腾讯安全御见威胁情报中心数据显示，上半年每周平均约23%的企业发生过终端病毒木马攻击事件，其中风险类软件感染占比最多（占40%），其次为后门远控类木马（占14%）。



员工终端安全

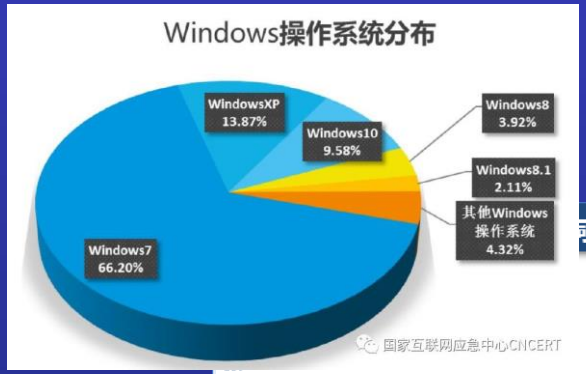
- 恶意软件

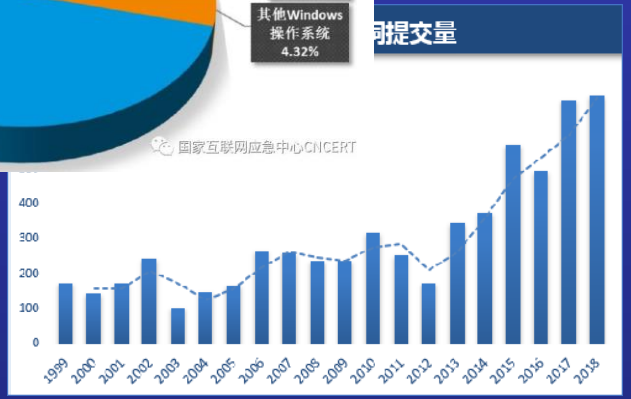
员工因非正规渠道下载到恶意的办公软件导致账号泄露、数据盗窃等安全问题。

员工终端安全

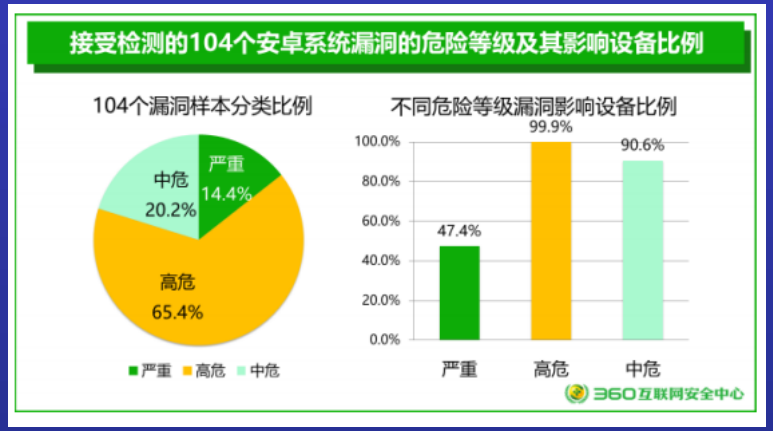
- 漏洞入侵

员工终端存在大量未修补的安全漏洞或危险配置，导致攻击者可以借此入侵破坏。





Windows
历年漏洞提交量



卸载也可开启摄像头监视：视频会议软件 Zoom Mac 版爆出严重安全漏洞

2019-07-10 10:37:29　16点赞　49收藏　41评论

员工终端安全

- 数据泄露

因为员工终端的维修、丢失等原因，导致存储到终端上的重要数据泄露。

第十名 德克萨斯大学马里兰州安德森癌症中心：430万美元

2018 年 6 月，法官维持了对德克萨斯大学 MD 安德森癌症中心因违反 HIPAA 规定而被罚款 430 万美元的决定。癌症中心在 2012 年至 2013 年间遭受了 3 次数据泄露，导致超过 33,500 个人的健康信息丢失。

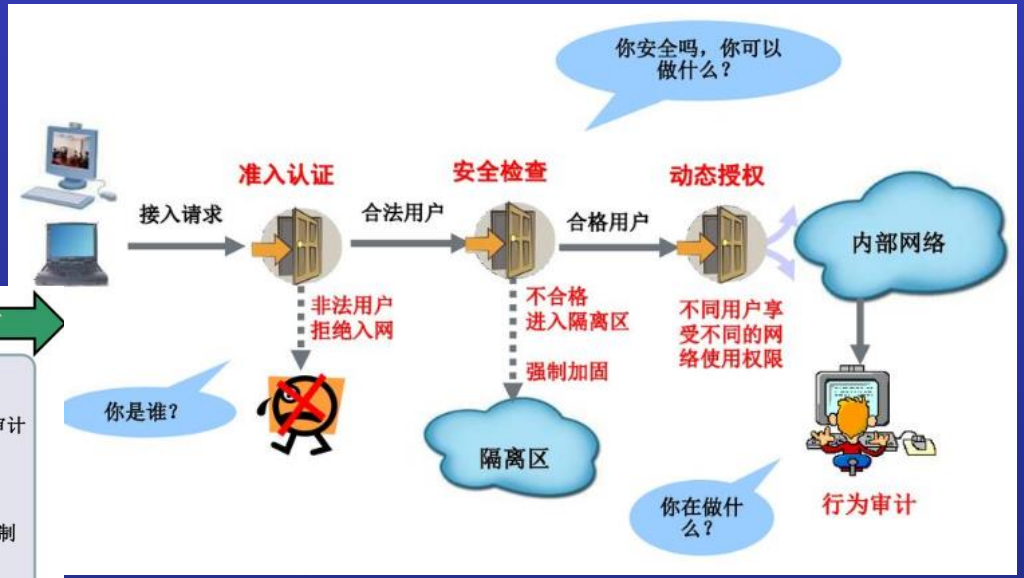
值得注意的是，三次数据泄露都是因为人员安全意识薄弱：有一次泄露是因为一台未加密的笔记本电脑从员工住所被盗。其他两次则是因为丢失未加密的 U 盘。

据外媒报道，Facebook未加密硬盘在工资管理部门的员工车内失窃，约2.9万名现任和前任雇员受到这起盗窃案的影响。

据Facebook周五上午与员工分享的电子邮件显示，这些未加密硬盘里的内容包括员工姓名、银行账号和社保号的最后四位数字等工资数据。此外，硬盘里还包含薪酬信息，比如工资、奖金金额和一些股权细节。

员工终端安全

- 对员工终端系统统一配发或者统一系统要求
- 购买或者自研对员工终端进行安全监控的程序实施安全管控和准入
- 终端安全必须和企业后端安全体系成一体来管理



员工终端安全

云桌面可以作为终端安全的选择方案

灵活访问

任何时间、任何地点、任何设备访问办公、业务环境
无需预先配置终端设备、安装应用客户端
平板电脑、智能手机同样可访问

保障安全

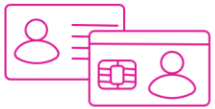
无需开放VPN，无需进入企业内网，保障内网安全
数据不外传，只传递指令不传递数据
水印、录像保障数据不外泄

简化运维

发布平台快速部署交付
终端设备、操作系统免维护
应用系统客户端集中部署、集中交付、集中运维

高质量用户体验

高清显示、流畅操作
与办公室桌面电脑完全一致的使用体验
浏览器访问，员工无需任何额安装配置



员工网络安全

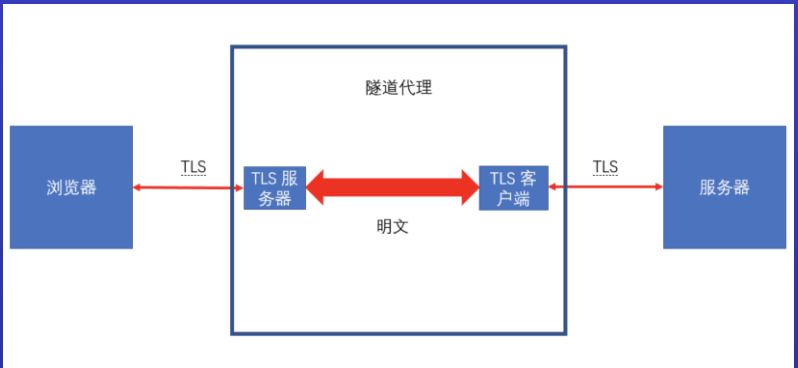
一般员工缺乏网络安全专业技能

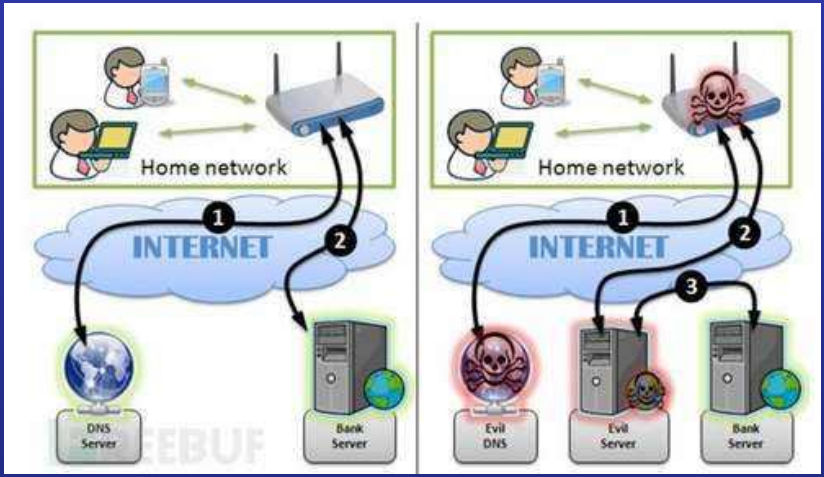
- 无法判断自己所使用的网络是否安全
- 无法对自己的家庭网络进行安全加固

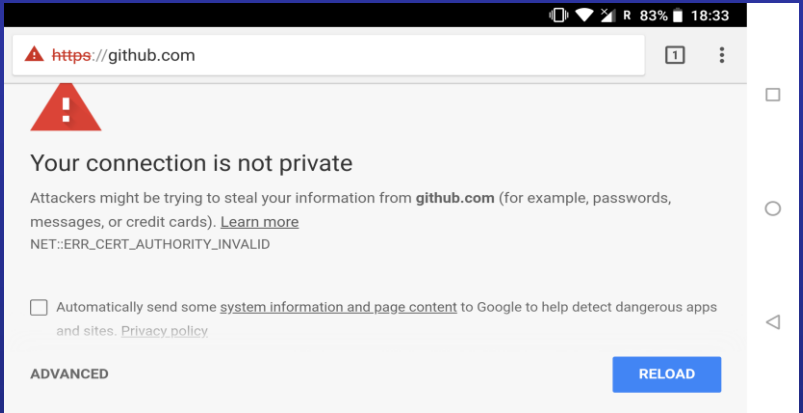
员工网络安全

- 链路劫持

坏人通过修改路由器配置等实现对员工网络链路的劫持进而攻击和盗窃。







员工网络安全

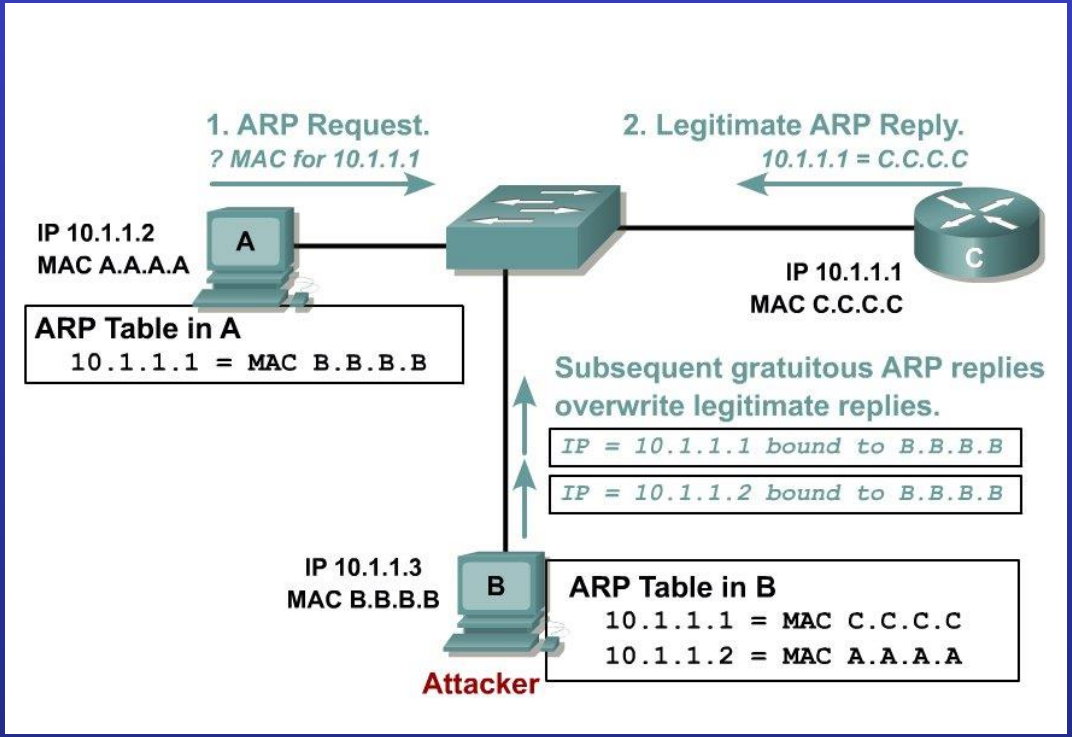
- 假冒网络

攻击者通过伪造公共WIFI等方式引诱员工连接到恶意网络从而进行攻击。

员工网络安全

- 网络嗅探

攻击者通过泄露的账号密码或入侵其他终端等方式进入到员工所在网络后通过抓包、网络欺骗等手段获取员工终端的通信数据，常见ARP欺骗、DHCP欺骗等。



员工网络安全

- 必须将员工网络视作不可信任主体来进行对待
  - 要结合终端安全、后端系统安全等来整体解决

强制员工使用VPN或者云桌面来访问公司系统

登录使用多媒介认证(譬如登录VPN使用固定密码+硬件令牌动态口令)

强制所有访问全程SSL(包括邮箱/网站等)

要求员工不要在公共网络进行进行敏感操作(可使用4G共享热点)

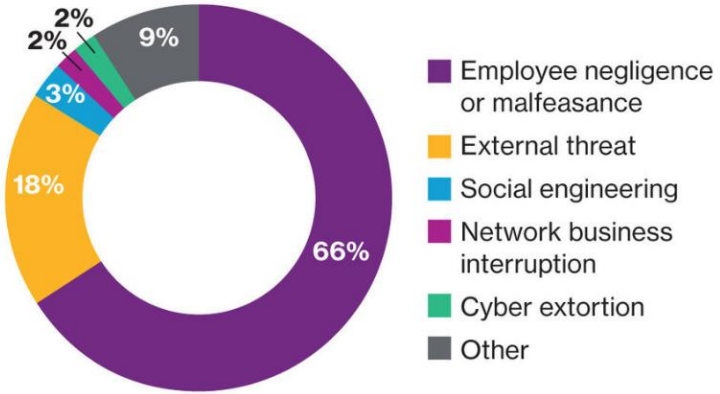
安装终端安全管控软件随时收集和监测员工网络情况

员工安全意识

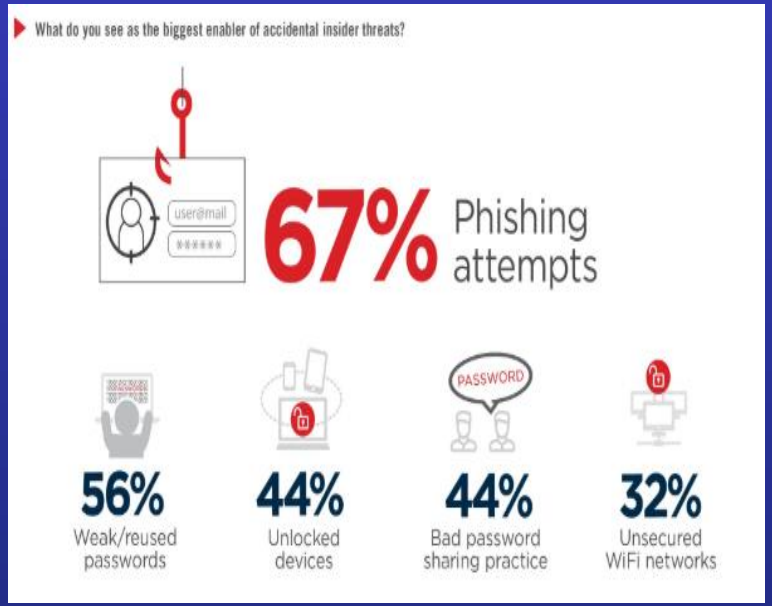
- 员工疏忽或者安全意识不足是造成网络安全事件的主因
- 远程办公的开放性进一步加剧员工问题导致安全事件概率

据著名国际咨询服务公司Willis Towers Watson的网络保险理赔数据显示，三分之二的网络安全漏洞问题是由于员工疏忽和渎职而直接或间接造成的。具体原因包括：电脑丢失、信息意外泄露、员工不良行为等。相较之下，仅有18%的网络安全问题是由外部威胁直接引发的。

Figure 1. **Percentage of claims by breach**



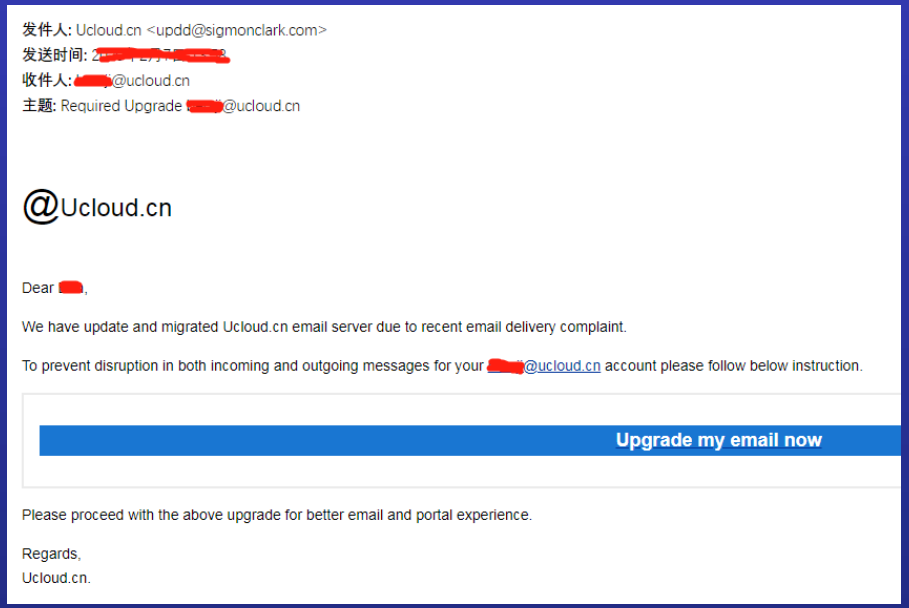
Source: Willis Towers Watson cyber insurance claims data



员工安全意识

- 钓鱼诈骗

攻击者伪造成员工信任的人/机构向员工发送邮件/短信/即时消息等，引诱员工访问恶意网站/安装恶意软件等，而且入侵员工电脑或者获得员工敏感信息。



员工安全意识

- 信息泄露

员工不恰当的分享或存储导致的信息泄露。


近日，据国外媒体报道，去年Uber曾遭受黑客攻击并导致数据大规模泄露。黑客通过第三方云服务对Uber实施了攻击，获取了5700万名用户数据，包括司机的姓名和驾照号码，用户的姓名、邮箱和手机号。

经过调查发现，数据泄露原因竟然是Uber解锁数据库的安全密钥被存储在GitHub的一个可以公开访问的页面。外媒称这是“In major goof”（超级傻瓜）的失误。

```
    "sync_down_on_open": true,
    "sync_same_age": true,

    "host": "c[redacted].kr",
    "user": "dcc120140248",
    "password": "mkw0268",
    //"port": "22",
    "upload_on_save":true,
    "remote_path": "/export/dcc_class/dcc/dcc120140248/hw1",
    //"file_permissions": "664",
    //"dir_permissions": "775",

    //"extra_list_connections": 0,
```

员工安全意识

- 危险操作

由于员工不安全的操作或配置导致安全事件发生

据外媒报道称，IT 安全和云数据管理公司 Rubrik 遭受了大规模数据泄露，遭到泄露的数据库托管在 Amazon Elasticsearch 服务器上，拥有数十亿字节的数据，泄露信息包括每个企业客户的客户名称、联系信息和工作信息。除此之外，数据库中还包含有来自企业客户的电子邮件，其中包含带有姓名、职位和电话号码的电子邮件签名，以及一些包含有关客户配置的敏感信息。

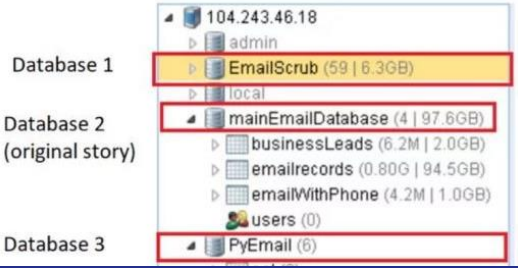
本次数据泄露事件是由安全研究员 Oliver Hough 发现的。2019 年 1 月 29 日，Rubrik 下线了该服务器，泄露事件发生的原因是暴露的服务器未受密码保护。

专家发现了一个不受保护的服务器公开了4个Verifications.io（电子邮件验证公司）在线MongoDB数据库（150GB），这些数据是营销公司的，内含多达8.09亿条记录。

这些数据是营销公司的，内含多达8.09亿条记录，包含：

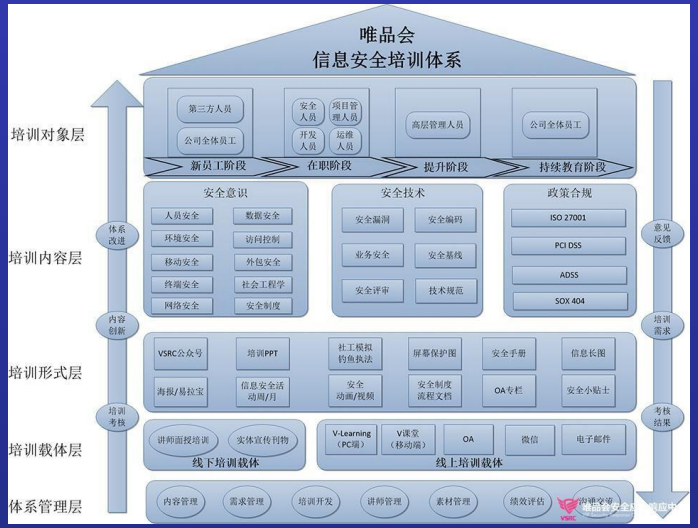
> 邮件记录= 798,171,891条记录
> emailWithPhone = 4,150,600条记录
> businessLeads = 6,217,358条记录

起初这些数据是在一个不受保护的数据库上发现，但后来网络安全公司Dynarisk宣布有4个数据库在网上泄露。



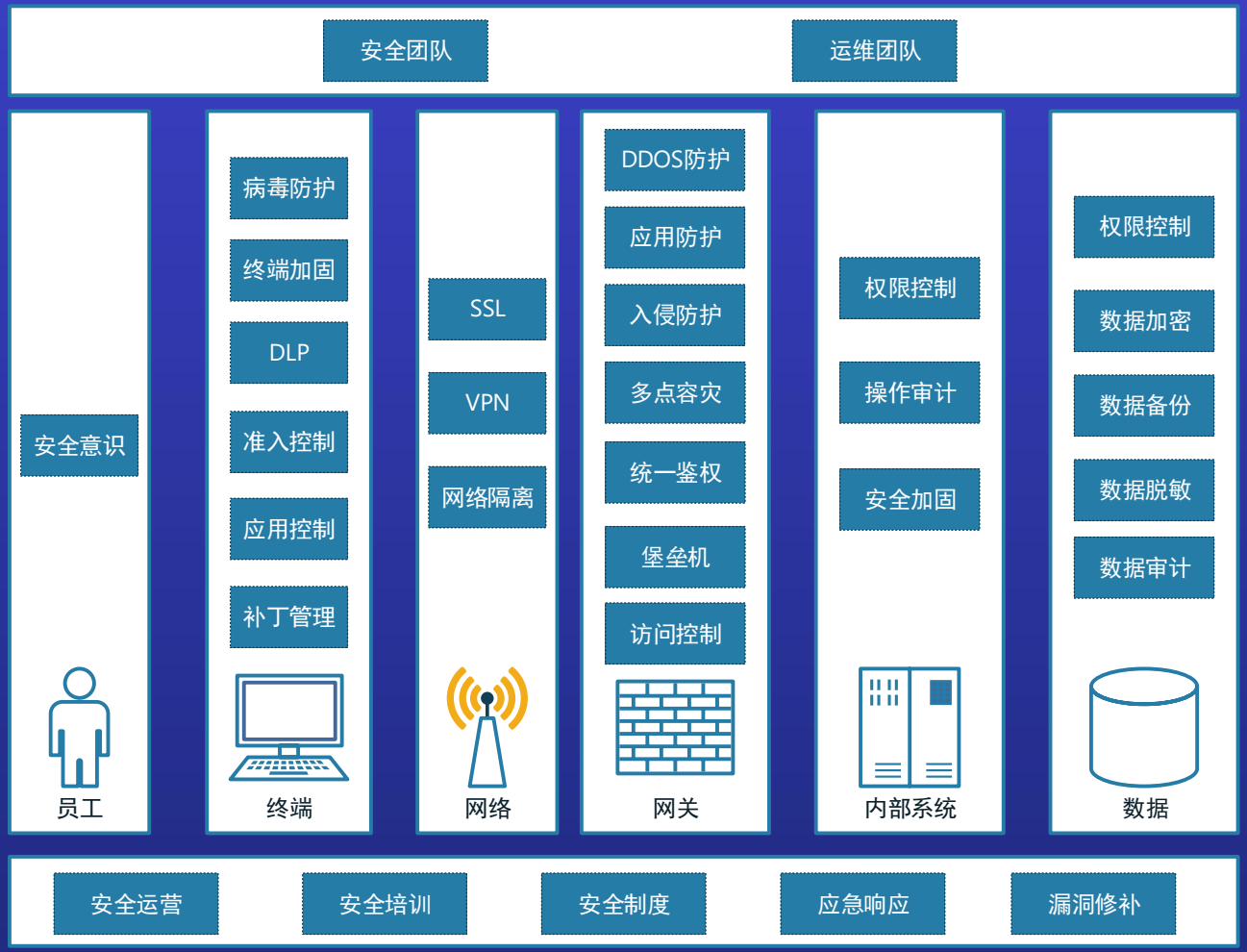
员工安全意识

- 员工具备良好安全意识可提升企业安全水平
- 培训是提升安全意识最有效途径
- 培训是必须是一个长期过程



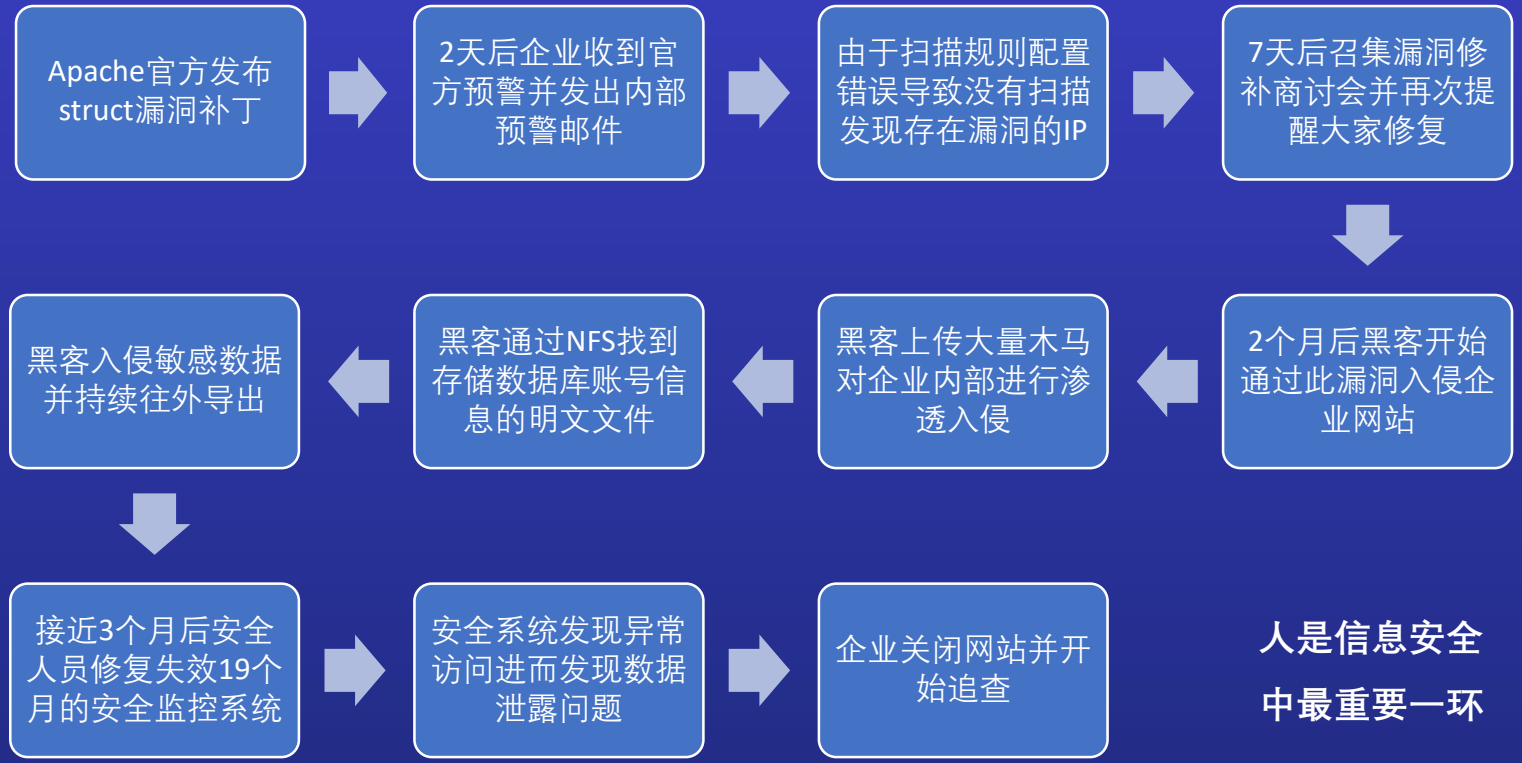
总结

远程办公安全概图


安全团队
运维团队
安全意识
员工
病毒防护
终端加固
DLP
准入控制
应用控制
补丁管理
终端
SSL
VPN
网络隔离
网络
DDOS防护
应用防护
入侵防护
多点容灾
统一鉴权
堡垒机
访问控制
网关
权限控制
操作审计
安全加固
内部系统
权限控制
数据加密
数据备份
数据脱敏
数据审计
数据
安全运营
安全培训
安全制度
应急响应
漏洞修补

总结

- 著名征信公司数据泄露事件给我们的启示



总结

- 远程办公的开放性导致了很多以前封闭内网办公未遇到的安全问题
- 企业必须对远程办公的所有环节(包括人和设备)都保持不信任原则
- 员工是信息安全中最重要的一环，一定要持续进行安全意识培养
- 远程办公的信息安全的各个环节，环环相扣、缺一不可
- 购买昂贵的安全系统，但没有员工配合、良好维护，一样没效果

Q&A

UCloud产品矩阵

跨物理机房的高可用网络

子网跨可用区可实现跨可用区灾备

跨可用区ULB/VIP等高可用产品

SSL证书	VPN网关	VPC	外网防火墙
证书服务， SSL证书极速签发 一键部署	高性能的IPSecVPN 网关	自定义网络空间 保证安全隔离	自定义安全策略 隔离公网威胁
堡垒机	数据库审计	主机入侵检测	数据方舟
操作审计产品 运维资产权限管理 保证运维安全	数据库操作审计 保证数据库数据安全	实时监控主机安全 辅助服务器加固	实时数据备份 确保数据安全
DDoS攻击防护	UWAF	UWS	态势感知
分布式立体DDoS 攻击防御解决方案	Web攻击拦截 分布式CC防御	Web漏洞扫描 提前修复漏洞	安全数据关联分析 威胁情报早知道

UCloud在行动

免费的云计算资源和技术服务支持

- 政务信息的及时同步
- 医疗信息同步
- 免费教育资源提供
- 在线医疗、物流、援助信息撮合、寻人系统等企业级用户

免费的云计算资源和技术服务支持

- 为无糖信息的“新型冠状感染性肺炎确诊患者相同行程查询系统”提供免费资源支持；
- UCloud志愿者开发团队研发浙江某地区口罩预约系统，助力防疫；
- 与多家教育机构紧密合作，力保全国师生“停课不停学”；
- 为北京大学可视化与可视分析实验室“新型冠状病毒感染肺炎疫情”的可视分析系统研发工作提供援助等，以科技之力，为全民战“疫”提供保障。

企业服务SaaS领域战疫扶持计划

- 面向SaaS产业联盟企业，UCloud提供免费2个月包括云主机、数据库、存储、CDN、安全、人工智能算力在内的基础云资源
- 加入UCloud “+U计划”，共享UCloud销售渠道资源
- 联合品牌&营销推广支持（UCloud免费为扶持伙伴引流）
- 官方网站、官方微信等推广落地页LOGO露出
- UCloud启云学院培训课程免费开放

注：提供的资源支持、扶持计划等均有上下文背景，具体信息以UCloud官网发布为准。

武汉加油！ 中国加油！

UCLOUD 优刻得

THANKS