schuelke.net
internet.security.consulting

Erkennungs- und Abwehrmöglichkeiten von Angriffen auf die Unternehmens-IT

Wiesbaden, 22.09.2015

Christian Schülke

schuelke.net – internet.security.consulting

Die Angreifer- und Bedrohungsseite

Zugang verschaffen

Festsetzen

Sichten

Sammeln

Herausbefördern

Aufbau und Ablauf eines Angriffs

Quelle: Dell Secure Works

Aufbau und Ablauf eines Angriffs

Quelle: Dell Secure Works

Schutzmechanismen
Erkennung von Angriffen

SANS Top20 - Description of Controls

(System Administration, Networking and Security)

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

SANS Top20 - Description of Controls

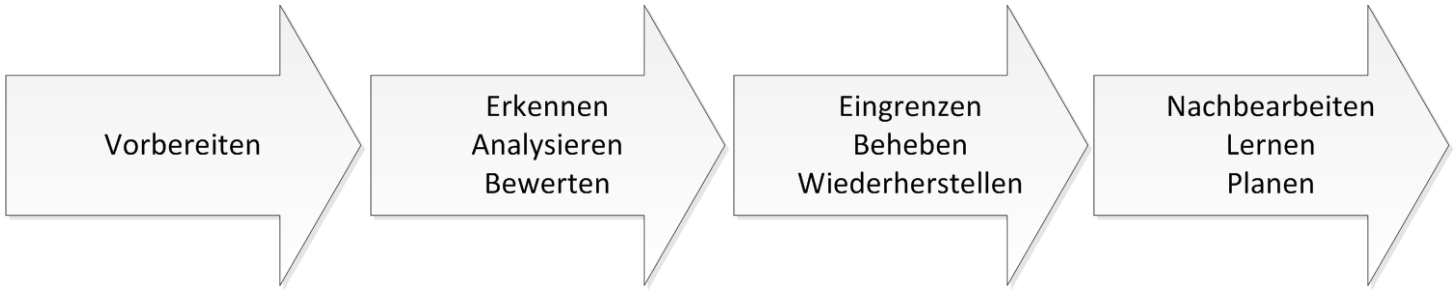
(System Administration, Networking and Security)

- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Top 15 ‚Indikatoren einer Kompromitierung‘

- Ungewöhnlicher ausgehender Netzwerk-Datenverkehr
- Unregelmäßigkeiten in Aktivitäten von privilegierten Accounts
- Geographische Unregelmäßigkeiten
- Andere Login Warnung
- Anschwellen von Datenbank Lese-Volumen
- HTML Response Sizes
- Hohe Anzahl Zugriffe auf die selbe Datei
- Untypische Port+Applikations-Kombination (Datenverkehr)
- Verdächtige Registry oder Systemfile Änderungen
- Unregelmäßigkeiten in DNS Anfragen
- Unerwartetes Patchen von Systemen
- Änderungen der Mobile Device Profile
- Datenmengen am falschen Ort
- Web Datenverkehr mit ‚nicht-menschlichem‘ Verhalten
- Anzeichen von dDoS Aktivitäten

Schematischer Ablauf der Incident-Behandlung



- Ohne Vorbereitung auf Incidents:

Start von Anfang an

- Mit Vorplanung, Schulung, Checklisten, etc.:

Schneller Einstieg in Analyse und Bewertung

- Mit Einsatz geeigneter technischer Unterstützung und Prozesse:

Direkte Gegenmaßnahmen

SIEM

SIEM

- Namensgebung:

S	I	E	M
System	Information	Event	Monitoring
Security	Incident		Management

- SIEM beschreibt die hohe Kunst, alle vorhandenen Daten aufzunehmen, zu korrelieren und hieraus Rückschlüsse auf bestimmte Ereignisse zu treffen

Beispiele für SIEM und Logging

- a) Loginformationen zentral vor dem versehentlichen/böswilligen Löschen sichern
- b) systemübergreifende Verhaltensmuster aufdecken
  - Bsp.: einzelne Falsch-Logins
  - Bsp.: Zugriffe auf eine Datenbank
- c) Benachrichtigung und Alarm
- d) automatische Reaktionen starten

Vielen Dank für Ihre Aufmerksamkeit!

schuelke.net
internet.security.consulting

schuelke.net – internet.security.consulting

Christian Schülke

Konrad-Adenauer-Str. 41

63225 Langen

www.schuelke.net | 06103-571 5571

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

FEBRUARY 2014

Strategies to Mitigate Targeted Cyber Intrusions

Introduction

1. Australian computer networks are being targeted by adversaries seeking access to sensitive information.

2. A commonly used technique is social engineering, where malicious "spear phishing" emails are tailored to entice the reader to open them. Users may be tempted to open malicious email attachments or follow embedded links to malicious websites. Either action can compromise the network and disclose sensitive information.

3. The Australian Signals Directorate (ASD), also known as the Defence Signals Directorate, has developed a list of strategies to mitigate targeted cyber intrusions. The list is informed by ASD's experience in operational cyber security, including responding to serious cyber intrusions and performing vulnerability assessments and penetration testing for Australian government agencies.

Mitigation Strategies

4. ASD's list of mitigation strategies, first published in February 2010, is revised for 2014 based on ASD's most recent analysis of cyber intrusions across the Australian Government. This document provides a summary of key changes for 2014.

5. While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 strategies remains very high. At least 85% of the cyber intrusions that ASD responds to involve adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

6. Implementing the Top 4 mitigation strategies can be achieved gradually, firstly on workstations of users who are most likely to be targeted by cyber intrusions, and then implementing them on all workstations and servers. Once this is achieved, organisations can selectively implement additional mitigation strategies to address security gaps until an acceptable level of residual risk is reached.

7. This document provides information about comparative mitigation implementation costs and user resistance levels to help organisations select the best set of strategies for their requirements.

8. These strategies complement the guidance provided in the *Australian Government Information Security Manual* (ISM) available on ASD's website.

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

Strategies to Mitigate Targeted Cyber Intrusions

Originally published 18 February 2010, updated for February 2014

Mitigation Strategy Effectiveness Ranking for 2014	(and 2012)	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1	(1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2	(2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3	(3)	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4	(4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategies can then be selected to address security gaps until an acceptable level of residual risk is reached.

5	(18)	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6	(N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7	(21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No
8	(11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9	(5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10	(7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11	(6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12	(8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13	(9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14	(10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15	(12)	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16	(13)	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17	(14)	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18	(15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible
19	(16)	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Yes	Yes	No	Yes
20	(19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21	(22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22	(25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23	(24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24	(23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25	(27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26	(29)	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	No	Yes	Possible	Yes
27	(28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28	(20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29	(26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30	(25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Possible	Possible	No	No
31	(30)	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	No	No	No	No
32	(32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33	(33)	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Possible	Possible	Possible	Possible
34	(34)	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Possible	Yes	No	Yes
35	(35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No

This document and additional information about implementing the 35 mitigation strategies is available at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

Summary of Key Changes for 2014

9. The *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details* document includes an annex of key changes for 2014. A summary of the most significant changes are as follows.

10. Mitigation strategy #4 'Restrict administrative privileges' has been amended to clarify that the goal of this strategy is to ensure that the only users who have administrative privileges to operating systems and applications such as databases, are those users who require such privileges based on their job role and duties.

11. Mitigation strategy 'User application configuration hardening' has moved from #18 to #5 to address intrusions that exploit the prevalence of Java vulnerabilities or involve malicious macro code in Microsoft Office files. Additional technical guidance is provided to enable organisations to continue using Java for business purposes while minimising their risk.

12. The newly introduced mitigation strategy #6 'Automated dynamic analysis' extracts the behavioural analysis functionality from the existing two mitigation strategies 'Email content filtering' and 'Web content filtering'. Additional technical guidance is provided to enable organisations to select an appropriate vendor product.

13. Mitigation strategy 'Operating system generic exploit mitigation' has moved from #21 to #7 due to the increased support and proven effectiveness of Microsoft's free "Enhanced Mitigation Experience Toolkit" (EMET) software tool at mitigating vulnerabilities that were not publicly known at the time.

14. The previous 'Antivirus software' mitigation strategy has been divided into two separate mitigation strategies, to highlight the difference between less effective signature-based antivirus software and more effective heuristic/anomaly-based antivirus software.

15. Mitigation strategy 'User education' has moved from #20 to #28 due to the increase in intrusions using techniques that an educated user would not detect.

Further Information

16. Additional supporting advice is available on the ASD website at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

Einführung und Hintergrund: SANS Top20 Critical Controls

Introduction: Critical Controls for Effective Cyber Defense

To secure against cyber attacks, organizations must vigorously defend their networks and systems from a variety of internal and external threats. They must also be prepared to detect and thwart damaging follow-on attack activities inside a network that has already been compromised. Two guiding principles are: "Prevention is ideal but detection is a must" and "Offense informs defense."

Benefits

- ***Quick wins*** that provide solid risk reduction without major procedural, architectural, or technical changes to an environment, or that provide such substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.
- ***Visibility and attribution*** *measures* to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.
- ***Improved information security configuration*** and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.
- ***Advanced sub-controls*** that use new technologies that provide maximum security but are harder to deploy or more expensive than commoditized security solutions.

Description of Controls

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

How Organizations Are Applying the Controls

Dozens of early adopters of the Critical Controls have shared their experiences and lessons learned with the Consortium for Cybersecurity Action (CCA). A pattern has emerged of steps common to many organizations that have made substantial progress in reducing risk using the Critical Controls:

- Step 1. Perform Initial Gap Assessment - determining what has been implemented and where gaps remain for each control and sub-control.
- Step 2. Develop an Implementation Roadmap - selecting the specific controls (and sub-controls) to be implemented in each phase, and scheduling the phases based on business risk considerations.
- Step 3. Implement the First Phase of Controls - identifying existing tools that can be repurposed or more fully utilized, new tools to acquire, processes to be enhanced, and skills to be developed through training.
- Step 4. Integrate Controls into Operations - focusing on continuous monitoring and mitigation and weaving new processes into standard acquisition and systems management operations.
- Step 5. Report and Manage Progress against the Implementation Roadmap developed in Step 2. Then repeat Steps 3-5 in the next phase of the Roadmap.

Action Plan

Given that these critical controls so closely track current threats and attacks, we recommend that CIOs and CISOs consider several immediate actions to ensure the effectiveness of their security programs:

1. Conduct a gap assessment to compare the organization's current security stance to the detailed recommendations of the Critical Controls
2. Implement the "First Five" and other "quick win" Critical Controls to address the gaps identified by the assessment over the next one or two quarters
3. Assign security personnel to analyze and understand how Critical Controls beyond the quick wins can be deployed in the organization's environment
4. Devise detailed plans to implement the "visibility and attribution" and "hardened configuration and improved information security hygiene" Critical Controls over the next year
5. Plan for deployment of the "advanced controls" over the longer term.

Attack Types vs. SANS top 20 Critical Cyber Security Controls

As described in the Introduction, numerous contributors who are responsible for responding to actual attacks or conducting red team exercises were involved in the creation of this document. The resulting Critical Controls are therefore based on first-hand knowledge of real-world attacks and the associated defenses.

Attack Summary	Most Directly Related Control
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	1
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines.	2, 3
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.	2, 4
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.	2, 10
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.	3, 10
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.	4, 5
Attackers compromise target organizations that do not exercise their defenses to determine and continually improve their effectiveness.	4, 5, 11, 20
Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools.	5, 15, 17
Attackers scan for remotely accessible services on target systems that are often unneeded for business activities, but provide an avenue of attack and compromise of the organization.	5, 10, 11
Attackers exploit weak application software, particularly web applications, through attack vectors such as SQL injection, cross-site scripting, and similar tools.	6, 20
Attackers exploit wireless access points to gain entry into a target organization's internal network, and exploit wireless client systems to steal sensitive information.	7
Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness.	9, 12, 16

Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.	10, 13
Attackers trick a user with an administrator-level account into opening a phishing-style e-mail with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine with full administrator privileges.	9, 12
Attackers exploit boundary systems on Internet-accessible DMZ networks, and then pivot to gain deeper access on internal networks.	13, 19
Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak filtering, or a lack of separation of important systems or business functions.	13, 19
Attackers operate undetected for extended periods of time on compromised systems because of a lack of logging and log review.	14
Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from nonsensitive information.	15, 17
Attackers compromise inactive user accounts left behind by temporary workers, contractors, and former employees, including accounts left behind by the attackers themselves who are former employees.	16
Attackers escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, which is then used to propagate to other victim machines across an enterprise.	12, 16
Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization.	17
Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information.	15, 17
Attackers operate undiscovered in organizations without effective incident-response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure production state.	18

Top 15 Indicators Of Compromise

Unusual account behaviors, strange network patterns, unexplained configuration changes, and odd files on systems can all point to a potential breach (Ericka Chickowski, October 09, 2013)

In the quest to detect data breaches more quickly, indicators of compromise can act as important breadcrumbs for security pros watching their IT environments. Unusual activity on the network or odd clues on systems can frequently help organizations spot attacker activity on systems more quickly so that they can either prevent an eventual breach from happening -- or at least stop it in its earliest stages.

According to the experts, here are some key indicators of compromise to monitor (in no particular order):

1. **Unusual Outbound Network Traffic**
2. **Anomalies In Privileged User Account Activity**
3. **Geographical Irregularities**
4. **Other Log-In Red Flags**
5. **Swells In Database Read Volume**
6. **HTML Response Sizes**
7. **Large Numbers Of Requests For The Same File**
8. **Mismatched Port-Application Traffic**
9. **Suspicious Registry Or System File Changes**
10. **DNS Request Anomalies**
11. **Unexpected Patching Of Systems**
12. **Mobile Device Profile Changes**
13. **Bundles Of Data In The Wrong Places**
14. **Web Traffic With Unhuman Behavior**
15. **Signs Of DDoS Activity**

1. Unusual Outbound Network Traffic
Perhaps one of the biggest telltale signs that something is amiss is when IT spots unusual traffic patterns leaving the network.

"A common misperception is that traffic inside the network is secure," says Sam Erdheim, senior security strategist for AlgoSec. "Look for suspicious traffic leaving the network. It's not just about what comes into your network; it's about outbound traffic as well."

Considering that the chances of keeping an attacker out of a network are difficult in the face of modern attacks, outbound indicators may be much easier to monitor, says Geoff Webb, director of solution strategy for NetIQ.

"So the best approach is to watch for activity within the network and to look for traffic leaving your perimeter," he says. "Compromised systems will often call home to command-and-control servers, and this traffic may be visible before any real damage is done."

2. Anomalies In Privileged User Account Activity
The name of the game for a well-orchestrated attack is for attackers to either escalate privileges of accounts they've already compromised or to use that compromise to leapfrog into other accounts with higher privileges. Keeping tabs on unusual account behavior from privileged accounts not only watches out for insider attacks, but also account takeover.

"Changes in the behavior of privileged users can indicate that the user account in question is being used by someone else to establish a beachhead in your network," Webb says. "Watching for changes -- such as time of activity, systems accessed, type or volume of information accessed -- will provide early indication of a breach."

3. Geographical Irregularities
Whether through a privileged account or not, geographical irregularities in log-ins and access patterns can provide good evidence that attackers are pulling strings from far away. For example, traffic between countries that a company doesn't do business with offers reason for pause.

"Connections to countries that a company would normally not be conducting business with [indicates] sensitive data could be siphoned to another country," says Dodi Glenn, director of security content management for ThreatTrack Security.

Similarly, when one account logs in within a short period of time from different IPs around the world, that's a good indication of trouble.

"As to data-breach clues, one of the most useful bits I've found is logs showing an account logging in from multiple IPs in a short time period, particularly when paired with geolocation tagging," says Benjamin Caudill, principal consultant for Rhino Security. "More often than not, this is a symptom of an attacker using a compromised set of credentials to log into confidential systems."

4. Other Log-In Red Flags
Log-in irregularities and failures can provide excellent clues of network and system probing by attackers.

"Check for failed logins using user accounts that don't exist -- these often indicate someone is trying to guess a user's account credentials and gain authorization," says Scott Pierson, product specialist for Beachhead Solutions, explaining that unusual numbers of failed log-ins for existing accounts should also be a red flag.

Similarly, attempted and successful log-in activity after hours can provide clues that it isn't really an employee who is accessing data.

"If you see John in accounting logging onto the system after work hours and trying to access files for which he is not authorized, this bears investigation," says A.N. Ananth, CEO of EventTracker.

5. Swells In Database Read Volume
Once an attacker has made it into the crown jewels and seeks to exfiltrate information, there will be signs that someone has been mucking about data stores. One of them is a spike in database read volume, says Kyle Adams, chief software architect for Junos WebApp Secure at Juniper Networks.

"When the attacker attempts to extract the full credit card database, it will generate an enormous amount of read volume, which will be way higher than you would normally see for reads on the credit card tables," he says.

6. HTML Response Sizes
Adams also says that if attackers use SQL injection to extract data through a Web application, the requests issued by them will usually have a larger HTML response size than a normal request.

"For example, if the attacker extracts the full credit card database, then a single response for that attacker might be 20 to 50 MB, where a normal response is only 200 KB," he says.

7. Large Numbers Of Requests For The Same File
It takes a lot of trial and error to compromise a site -- attackers have to keep trying different exploits to find ones that stick. And when they find signs that an exploit might be successful, they'll frequently use different permutations to launch it.

"So while the URL they are attacking will change on each request, the actual filename portion will probably stay the same," Adams says. "So you might see a single user or IP making 500 requests for 'join.php,' when normally a single IP or user would only request that page a few times max."

8. Mismatched Port-Application Traffic
Attackers often take advantage of obscure ports to get around more simple Web filtering techniques. So if an application is using an unusual port, it could be sign of command-and-control traffic masquerading as "normal" application behavior.

"We have noticed several instances of infected hosts sending C&C communications masked as DNS requests over port 80," says Tom Gorup, SOC analyst for Rook Consulting. "At first glance, these requests may appear to be standard DNS queries; however, it is not until you actually look at those queries that you see the traffic going across a nonstandard port. "

9. Suspicious Registry Or System File Changes
One of the ways malware writers establish persistence within an infected host is through registry changes.

"Creating a baseline is the most important part when dealing with registry-based IOCs," Gorup says. "Defining what a clean registry is supposed to contain essentially creates the filter against which you will compare your hosts. Monitoring and alerting on changes that deviate outside the bounds of the clean 'template' can drastically increase security team response time."

Similarly, many attackers will leave behind signs that they've tampered with a host in system files and configurations, says Webb, who has seen organizations more quickly identify compromised systems by looking for these kinds of changes.

"What can happen is that the attacker will install packet-sniffing software to harvest credit card data as it moves around the network," he says. "The attacker targets a system that can watch the network traffic, then installs the harvesting tool. While the chances of catching the specific harvesting tool are slim -- because they will be targeted and probably not seen before -- there is a good chance to catch the changes to the system that houses the harvesting tool."

10. DNS Request Anomalies
According to Wade Williamson, senior security analyst for Palo Alto Networks, one of the most effective red flags an organization can look for are telltale patterns left by malicious DNS queries.

"Command-and-control traffic is often the most important traffic to an attacker because it allows them ongoing management of the attack and it needs to be secure so that security professionals can't easily take it over," he says. "The unique patterns of this traffic can be recognized and is a very standard approach to identifying a compromise."

Gorup agrees that DNS exfiltration can be "extremely loud."

"Seeing a large spike in DNS requests from a specific host can serve as a good indicator of potentially suspect activity," he says. "Watching for patterns of DNS requests to external hosts, compared against geoIP and reputation data, and implementing appropriate filtering can help mitigate C&C over DNS."

11. Unexpected Patching Of Systems
Patching is generally a good thing, but if a system is inexplicably patched without reason, that could be the sign that an attacker is locking down a system so that other bad guys can't use it for other criminal activity.

"Most attackers are in the business of making money from your data -- they certainly don't want to share the profits with anyone else," Webb says. "It sometimes does pay to look security gift horses in the mouth."

12. Mobile Device Profile Changes
As attackers migrate to mobile platforms, enterprises should keep an eye on unusual changes to mobile users' device settings. They also should watch for replacement of normal apps with hostile ones that can carry out man-in-the-middle attacks or trick users into giving up their enterprise credentials.

"If a managed mobile device gains a new configuration profile that was not provided by the enterprise, this may indicate a compromise of the user's device and, from there, their enterprise credentials," says Dave Jevans, founder and CTO of Marble Security. "These hostile profiles can be installed on a device through a phishing or spear-phishing attack."

13. Bundles Of Data In The Wrong Places
According to EventTracker's Ananth, attackers frequently aggregate data at collection points in a system before attempting exfiltration.

"If you suddenly see large gigabytes of information and data where they should not exist, particularly compressed in archive formats your company doesn't' use, this is a telltale sign of an attack," he says.

In general, files sitting around in unusual locations should be scrutinized because they can point to an impending breach, says Matthew Standart, director of threat intelligence at HBGary.

"Files in odd places, like the root folder of the recycle bin, are hard to find looking through Windows, but easy and quick to find with a properly crafted Indicator of Compromise [search]," Standart says. "Executable files in the temp folder is another one, often used during privilege escalation, which rarely has a legitimate existence outside of attacker activity."

14. Web Traffic With Unhuman Behavior
Web traffic that doesn't match up with normal human behavior shouldn't pass the sniff test, says Andrew Brandt, director of threat research for Blue Coat.

"How often do you open 20 or 30 browser windows to different sites simultaneously? Computers infected with a number of different click-fraud malware families may generate noisy volumes of Web traffic in short bursts," he says." Or, for instance, on a corporate network with a locked-down software policy, where everyone is supposed to be using one type of browser, an analyst might see a Web session in which the user-agent string which identifies the browser to the Web server indicates the use of a browser that's far removed from the standard corporate image, or maybe a version that doesn't even exist."

15. Signs Of DDoS Activity
Distributed denial-of-service attacks (DDoS) are frequently used as smokescreens to camouflage other more pernicious attacks. If an organization experiences signs of DDoS, such as slow network performance, unavailability of websites, firewall failover, or back-end systems working at max capacity for unknown reasons, they shouldn't just worry about those immediate problems.

"In addition to overloading mainstream services, it is not unusual for DDoS attacks to overwhelm security reporting systems, such as IPS/IDS or SIEM solutions," says Ashley Stephenson, CEO at Corero Network Security. "This presents new opportunities for cybercriminals to plant malware or steal sensitive data. As a result, any DDoS attack should also be reviewed for related data breach activity."

Link to original article: http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/240162469?pgno=1