ALE | Where Everything Connects

Campus-Cybersicherheit in Zeiten von IOT und DSGVO

Alcatel·Lucent Enterprise

Inhaltsverzeichnis

Einführung

Die Campus-Cybersicherheit ist seit Jahren ein Thema mit höchster Priorität im Hochschulwesen. Zum zweiten Mal innerhalb drei Jahren nimmt die Informationssicherheit den Topplatz ein in der jährlichen Educause-Umfrage unter den Hochschul-CIOs zu den 10 wichtigsten IT-Problemen[1]. Schaut man sich die Ergebnisse des neuesten Verizon Data Breach Investigations Report (DBIR) an, verwundert dies wenig[2]. Der Bericht vermeldet bei cyberkriminellen Aktivitäten einen deutlichen Aufwärtstrend und zeigt die 3 gefährdetsten Branchen klar auf: Finanz, Gesundheit und Bildung.

Die Informationssicherheit im Bildungsbereich steht seit jeher im Spannungsfeld zwischen Benutzerfreundlichkeit und Sicherheit. Manchmal überwiegt die Sicherheit, aber meistens liegt die Priorität doch bei der Benutzerfreundlichkeit. Angesichts der neuen europäischen Datenschutzgesetzgebung, zusammengefasst in der sogenannten Datenschutzgrundverordnung[3, 4] (DSGVO), und der Vielzahl neu eingeführter IoT-Geräte, überrascht es nicht, dass die Themen Informationssicherheit und Reputationsschutz ihrer Einrichtungen ganz oben auf der Agenda der Hochschul-CIOs stehen.

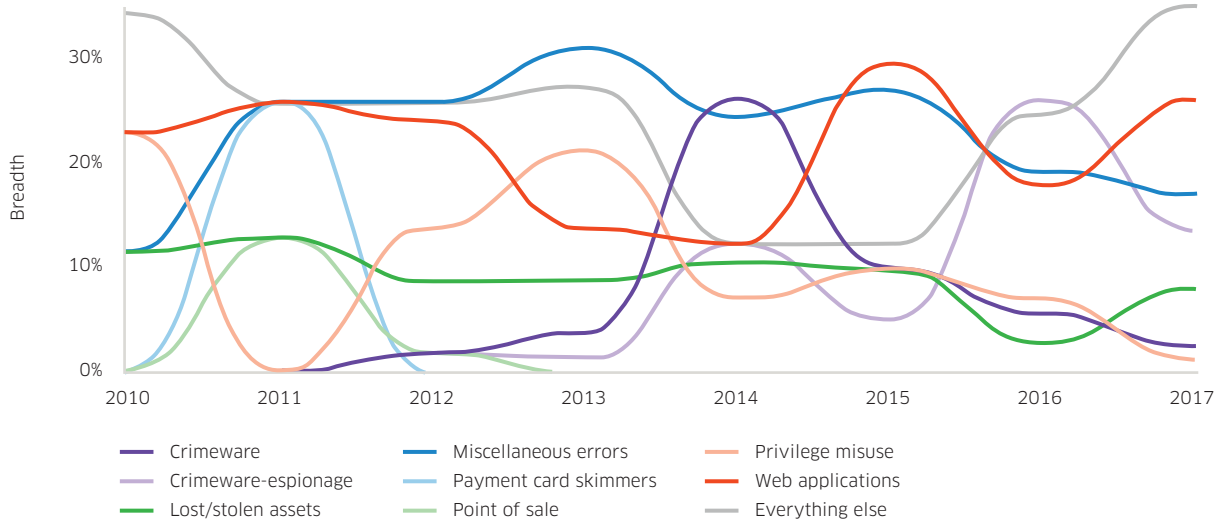
Der Fokus auf Informationssicherheit ist jedoch auch mehr als zeitgenmäß. Noch nie hat die Informationstechnologie eine so wichtige Rolle im Bildungsbereich gespielt wie heute. Ob es um Themenrecherchen für eine Vorlesung oder das Einreichen von Seminararbeiten geht – die IT und die implementierten Strategien zur Ermittlung und Sicherung des akademischen Erfolgs der Studierenden sind Kernelemente der Hochschulaktivitäten.

Der Verizon Data Breach Investigations Report 2018 enthält hierzu einige sehr interessante Erkenntnisse über die Angriffsvektoren und Motive für missbräuchliche Cyberaktivitäten.

Tabelle 1. Übersicht über Datensicherheitsverletzungen im Bildungswesen in 2017

Häufigkeit	292 Vorfälle, davon 101 mit bestätigter Offenlegung von Daten
Top-3-Angriffsmuster	76 % aller Sicherheitsverletzungen fallen unter die Kategorien „Alle sonstigen“, „Web-App-Angriffe“ und „Verschiedene Fehler“.
Bedrohungsakteure	Externe (81 %), Interne (19 %), Partner (2 %), Mehrere Akteure (2 % der Sicherheitsverletzungen)
Motive der Akteure	Finanzielle Gründe (70 %), Spionage (20 %), Spaß (11 %)
Kompromittierte Daten	72 % persönliche, 14 % vertrauliche und 11 % medizinische Daten

Abbildung 1. Muster von Sicherheitsverletzungen in Bildungseinrichtungen



1 EDUCAUSE Center for Analysis and Research (ECAR), “Top 10 IT Issues 2018,” EDUCAUSE Research Snapshot, EDUCAUSE Review, 29. Januar 2018.

2 Verizon Enterprise, “Verizon Data Breach Investigations Report (DBIR) 2018”, April 2018, Seite 29-30

3 https://eugdpr.org

4 https://gdpr-info.eu

Dieses Whitepaper untersucht den Stand der Implementierung von risikobasierten Sicherheitsstrategien wie dem Konzept der tief gestaffelten Verteidigung (Defense-in-Depth). Bei diesem Konzept wird das Computernetzwerk durch eine Reihe von einzelnen Verteidigungsmechanismen geschützt, sodass ein Angreifer erst mehrere, voneinander unabhängige Ebenen überwinden muss, um Erfolg zu haben.

In diesem Dokument wird häufig auf die „CIA-Triade" Bezug genommen. Dieser Begriff dient zur Einstufung von Angriffen auf die Vertraulichkeit („Confidentiality"), die Integrität („Integrity") oder die Verfügbarkeit („Availability") von Informationen. Die CIA-Triade ist insbesondere bei der Formulierung von campusweiten Sicherheitsrichtlinien und der Risikobewertung von Bedeutung. Beispielsweise wird der Diebstahl oder Verlust eines Laptops, auf dem personenbezogene Daten (PII) gespeichert sind, als Verletzung von vertraulichen Informationen eingestuft. Ein Hacker, der Prüfungsnoten verändert, schädigt die Integrität des Studenteninformationssystems. Und wenn ein BYOD-Drucker in einem Wohnheim für einen Denial of Service-Attacke (DoS) missbraucht wird, ist dies ein Angriff auf die Verfügbarkeit von Informationen, da das Ziel eines DoS-Angriffs darin besteht, einen Webserver mit so vielen falschen Anfragen zu überfluten, dass er nicht mehr auf legitime Anfragen reagieren kann.

Im Rahmen dieses Dokuments werden Bedrohungen der Informationssicherheit allgemein als missbräuchliche Cyberaktivitäten bezeichnet, die von der US-Regierung folgendermaßen definiert werden:

> „Aktivitäten, die nicht gemäß US-Recht erlaubt sind und darauf abzielen, die Vertraulichkeit, Integrität oder Verfügbarkeit von Computern, Informations- und Kommunikationssystemen, Netzwerken, durch Computer oder Informationssysteme gesteuerten physischen oder virtuellen Infrastrukturen oder der darin gespeicherten Daten zu beeinträchtigen oder beschädigen."

Folgen missbräuchlicher Cyberaktivitäten können sein:

> „Die Manipulation, Unterbrechung, Außerbetriebsetzung, Leistungsverschlechterung oder Zerstörung von Computern, Informations- und Kommunikationssystemen, Netzwerken, durch Computer oder Informationssysteme gesteuerten physischen oder virtuellen Infrastrukturen oder der darin gespeicherten Daten."

Das Jahr 2018 markierte einen Wendepunkt, angesichts der Flut von Internet-of-Things-Geräten (IoT) auf dem Campus und der Einführung neuer Datenschutzvorschriften im Internet, insbesondere der EU-Datenschutzgrundverordnung (DSGVO). Die DSGVO hat erhebliche Auswirkungen auf Universitäten weltweit und beide Themen werden hier ausführlich besprochen.

Datenschutzgrundverordnung (DSGVO)

Die DSGVO wurde am 25. Mai 2018 von der Europäischen Union in Kraft gesetzt, um den Bürgern die Kontrolle über ihre persönlichen Daten zurückzugeben. Im Wesentlichen gewährt die DSGVO jedem EU-Bürger das Recht, zu wissen und zu bestimmen, wie seine personenbezogenen Daten verwendet, gespeichert, geschützt, übertragen und gelöscht werden. Einzelpersonen steht auch das „Recht auf Vergessenwerden" zu, indem sie verlangen können, dass alle ihre Daten gelöscht werden. Im Gegensatz zur Definition personenbezogener Daten in anderen Ländern gilt die DSGVO auch für Standortdaten einschließlich IP-Adressen – was erhebliche Auswirkungen auf die Bereitstellung von standortbezogenen Diensten (Location Based Services, LBS) auf dem Campus und selbst auf die von Netzwerkkomponenten erstellten Protokolle haben kann..

Als fortschrittlichstes Datenschutzgesetz der Welt hat die DSGVO zusätzlich zu den oben dargelegten Rechten auch die Befugnis zur Sanktionierung bei Nichterfüllung. Verstöße gegen die DSGVO können Strafzahlungen in Höhe von 4 % des weltweiten Jahresumsatzes oder 23 Millionen US-Dollar nach sich ziehen – je nachdem, welcher Betrag höher ist.

Eine DSGVO-gerechte Planung zählt zur Kategorie „Vertraulichkeit" der CIA-Triade und wird im Abschnitt „Anwendungssicherheit" erläutert.

Internet of Things (IoT)

Das Internet der Dinge (Internet of Things, IoT) ist ein hochinteressantes Thema. Im Gegensatz zum Software-Defined Networking (SDN), das eine konsistente Implementierung durch die Networking-Community voraussetzt, sind IoT-Geräte bereits auf dem Campus vorhanden und und die Zahl wächst kontinuierlich. Ein IoT-Gerät ist ein vernetztes Gerät, das die Fähigkeit besitzt, Informationen zu senden und zu empfangen, ohne dass menschliche Eingriffe erforderlich sind. Typische IoT-Geräte auf einem Campus sind z. B. private WLAN-Drucker, Überwachungskameras und IoT-Sensoren oder auch Projektoren in Hörsälen und Seminarräumen.

Im Rahmen der normalen Nutzung sind diese Geräte eigentlich harmlos. Doch da sie vernetzt sind und ein Betriebssystem haben, sind sie anfällig für Hacker und Malware – und somit der Gefahr ausgesetzt, für feindliche Zwecke missbraucht zu werden. Vielleicht erinnern Sie sich noch an die DDoS-Attacke (Distributed Denial-of-Service) von Oktober 2016[5] gegen Dyn, einen Domain-Name-Service-Anbieter in den USA mit Kunden in Europa und Nordamerika. Dyn wurde an einem Tag dreimal angegriffen. Die daraufhin durchgeführte Analyse bestätigte, dass IoT-Geräte (Kameras, Babyüberwachungsgeräte, WLAN-Router und Drucker) mit einer Malware-Variante auf Basis des Mirai- Virenquellcodes infiziert waren.

Planungen für das IoT gehören überwiegend in die Kategorie „Verfügbarkeit“ der CIA-Triade und werden im Bereich Netzwerkzugriffssicherheit besprochen.

Defense in Depth (Tief gestaffelte Verteidigung)

Defense in Depth ist ein Verfahren zur Verteidigung eines Computers mit voneinander unabhängigen Sicherheitsvorkehrungen oder -strategien auf mehreren Ebenen. Es wurde ursprünglich von der US National Security Agency (NSA) als umfassendes Konzept zum Schutz von Informationen entwickelt. Das Konstrukt beruht auf drei Schwerpunkten:

1. Personen: Informationssicherung (Information Assurance) ist das übergeordnete Ziel der ITFührung und umfasst die Anwendung von Services zum Schutz der Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit und Nichtabstreitbarkeit der Urheberschaft. Die Anwendung dieser Services muss dem Paradigma „Schützen, Erkennen und Reagieren“ entsprechen. In diesen Bereich fallen auch Einstellungs- und Freistellungspraktiken sowie Schulungen
2. Technologie: Umfasst Hardware und Software, die den Zugriff auf die Inhalte eines Systems verhindern.
3. Betrieb: Befasst sich mit allen Aktivitäten, die zur alltäglichen Aufrechterhaltung der Sicherheitslage einer Organisation erforderlich sind, und beinhaltet Vorgänge wie Systemsicherheitsbewertungen, Wiederherstellung und Rekonstitution, Änderungssteuerung und Datenhandling.

In den folgenden Abschnitten des Whitepapers werden diese Schwerpunkte auf folgenden Ebenen untersucht: Netzwerk-Edge-Sicherheit, Anwendungssicherheit, Netzwerk-LAN-Sicherheit, Netzwerksegmentierung und Netzwerkmanagement.

Netzwerk-Edge-Sicherheit

„Edge“ ist der Punkt am Rand des Netzwerks, an dem das interne Netzwerk der Institution mit einem externen Netzwerk verbunden wird, z. B. dem Telefonnetz, einem Forschungs- und Bildungsnetzwerk oder dem öffentlichen Internet. Dies ist die erste Verteidigungsebene in einer Defense-in-Depth-Architektur. Damit sorgt diese Ebene sozusagen für den Schutz der Informationssicherheit vor den den „Angreifern vor dem Tor“ und ihren Absichten.

Da am Randbereich des Netzwerks sowohl eingehender als auch ausgehender Datenverkehr fließt, müssen beide Arten des Datenverkehrs berücksichtigt werden.

5 https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

Eingehender Datenverkehr

Unabhängig davon, ob der eingehende Datenverkehr über eine WAN-Verbindung, das öffentliche Internet oder eine Forschungsnetzwerk-Anbindung ankommt, sollten einige oder alle der folgenden Technologien angewendet werden:

1. Firewall: Die normalerweise in der DMZ (Demilitarized Zone) installierte Firewall erfüllt mehrere Sicherheitsaufgaben, darunter NAT (Network Address Translation), VPN (Virtual Private Network) und natürlich die Anwendung der Sicherheitslogik auf den Datenverkehr.
2. Intrusion Detection System (IDS) / Intrusion Detection and Prevention System (IDP): Wichtige Vorkehrungen zum Schutz des Netzwerks vor Angriffen. Es gibt zwei Typen:
    1) Signaturbasierte Systeme, die Muster von bekannten Exploits erkennen
    2) Anomaliebasierte Systeme, die Abweichungen von der standardmäßigen Netzwerkaktivität erkennen
3. Virtual Private Network (VPN): Stellt eine verschlüsselte Verbindung mit dem lokalen Netzwerk bereit. Dieser Verbindungstyp ist der beste für sichere Kommunikation und verwendet normalerweise ein Multifaktor-Authentifizierungssystem (MFA).
4. SPAM-Filter: Gelten vielfach als eine E-Mail-Server-Firewall. SPAM-Filter sind erheblich raffinierter geworden und besitzen Fähigkeiten zur Erkennung von Malware-infizierten Anhängen, gefälschten Adressen (Phishing) und anderen Arten von Angriffen. Laut dem Verizon Data Breach Report ist Phishing einer der Hauptangriffsvektoren im Hochschulwesen. Durch Implementierung eines SPAM-Filters lässt sich die Anzahl von Angriffen deutlich reduzieren.
5. Web-Traffic-Filter: Diese Aufgabe wird von manchen Firewalls mitübernommen und nicht alle Institutionen haben Web-Traffic-Filter implementiert. Mithilfe dieser Technologie können Universitäten jedoch den Zugriff auf Websites aus ihrem Netzwerk zulassen oder verweigern. Diese Sicherheitsvorkehrung, die vorwiegend in Schulen zur Anwendung kommt, hält Benutzer von gefährlichen Websites fern, die Vireninfektionen oder Kontrollverlust verursachen können.
6. Netzwerksicherheits-Überwachung: Anwendungen wie Bro[6] oder Splunk[7] liefern aufschlussreiche Daten zum Datenverkehr im Netzwerk und zu potenziellen Sicherheitsanomalien.

Ausgehender Datenverkehr

Netzwerke fordern nicht nur Datenverkehr an, sondern senden auch Daten nach außen. Auch wenn diese Art des Datenverkehrs normalerweise unverdächtig ist, kann dessen Überwachung dazu beitragen, dass die Institution bei einer Sicherheitsverletzung (z. B. wenn mit Malware infizierte IoTGeräte an einem DDoS-Angriffe teilnehmen) frühzeitig gewarnt wird.

Ausgehender Verkehr muss die Verteidigungsvorkehrungen für eingehenden Datenverkehr durchlaufen. Es gibt jedoch eine nützliche Methode zum Schutz des ausgehenden Verkehrs – Verschlüsselung.

1. Die MACSec-Verschlüsselung ist auch unter IEEE-Bezeichnung 802.1AE bekannt. Diese Technologie unterstützt verschlüsselte Übertragungen über eine Verbindung. Wenn zum Beispiel ein Disaster-Recovery-Standort (DR) für Ihr Rechenzentrum eingerichtet ist, können Sie Ihre Daten über eine MACSec-verschlüsselte Verbindung an diesen Standort senden, um Datenvertraulichkeit, Datenintegrität und Authentizität des Datenursprungs zu gewährleisten..

Anwendungssicherheit

Die nächste Ebene bei der Abwehr heutiger Cybersicherheitsbedrohungen ist die Anwendungssicherheit. Diese Ebene umfasst sowohl Endnutzer-Computer als auch netzwerkbasierte Anwendungen. Anwendungssicherheit ist ein wichtiges Werkzeug im Sicherheitsarsenal einer Universität. Es deckt die Bereiche Vertraulichlichkeit und Integrität der CIA-Triade ab und ist bei der Implementierung von DSGVO-Schutzmaßnahmen unbedingt zu berücksichtigen.

6 https://www.bro.org
7 https://www.splunk.com

Wichtige Technologien und Taktiken auf dieser Ebene:

1. Datenverschlüsselung: Beide großen PC-Betriebssysteme verfügen über Verschlüsselungsfunktionen für Festplattendaten. Diese wichtige Technologie schützt die Benutzerdaten vor spontanem Zugriff. Auch der Einsatz von Netzwerkspeicher-Verschlüsselung nimmt immer mehr zu und sorgt für besseren Schutz der Integrität und Vertraulichkeit der Informationen.
2. Multifaktor-Authentifizierung (MFA): Bei der Multifaktor-Authentifizierung müssen zwei Geräte parallel genutzt werden, damit der Zugriff auf eine Anwendung oder Ressource freigegeben wird. In der Regel ist der Ablauf so, dass nach Eingabe von Benutzer-ID und Passwort eine SMS mit einer Zahlenfolge an das Smartphone des Benutzers gesendet wird. Dadurch wird eine zusätzliche Bestätigungsebene geschaffen, um sicherzustellen, dass die Person diejenige ist, als die sie sich bezeichnet. Eine weitere Methode zur MFA-Bereitstellung ist die Verwendung von Hardware-Token, z. B. RAS und Google, anstelle einer Smartphone-SMS. Diese Strategie hat den Vorteil, dass sie auch in VPN und anderen Strategien für sichere Kommunikation genutzt werden kann..
3. Mikrosegmentierung: Im Rechenzentrum werden physische Server zunehmend durch virtuelle Server ersetzt. Auf der Stellfläche von einem oder zwei physischen Servern können Dutzende von virtuellen Servern untergebracht werden. Doch diese Dichte bringt auch Risiken mit sich. Traditionelle Stateful-Inspection-Firewalls sind nicht imstande, Datenverkehrsströme in einem Rechenzentrum mit Leitungsgeschwindigkeit zu analysieren. Der bekannte Hypervisor-Anbieter VMWare[8] hat eine Technologie namens „Mikrosegmentierung“ eingeführt. Mit dieser Technologie kann jede Anwendung einen eigenen Sicherheitsperimeter haben, ohne dass ausschließlich VLANs verwendet werden müssen.

Empfehlenswerte Sicherheitsmaßnahmen auf dieser Ebene:

4. Sicherheitsbewusstseins-Training für Endnutzer: Diese Aktivität wird üblicherweise im „Monat des Sicherheitsbewusstseins“ (Oktober) durchgeführt. Es sollten jedoch auch im Laufe des Jahres regelmäßig Erinnerungen bezüglich Phishing-, Spear-Phishing- und Social-Engineering-Angriffen (Offenlegen von Anmeldeinformationen) ausgegeben werden, um die Angriffsfläche zu verringern.
5. Sicherheitspatches: Es hat sich bewährt, Sicherheitspatches und Anwendungsupdates immer zu testen, bevor sie angewendet werden. Neue Releases vom Hersteller sind jedoch wichtig und sollten priorisiert werden. Laut der Verizon Data Breach-Studie wurden bei 6 % der erfolgreichen Angriffe Sicherheitslücken ausgenutzt, die durch einen Patch abgedeckt worden wären. Einige der verheerendsten Attacken sind tatsächlich durch eine verspätete Patch Anwendung zustande gekommen!

Netzwerkzugriffsicherheit

Local Area Networks (LAN) und Wireless Local Area Networks (WLAN) sind Eingangstore für die Computing-Benutzer auf dem gesamten Campus. Zum Herstellen einer LAN-Verbindung wird normalerweise ein Netzwerkgerät mit einem Ethernet-Patchkabel an einer RJ-45-Wandsteckdose angeschlossen. Eine WLAN-Verbindung erfordert keine physische Konnektivität, sondern nutzt stattdessen den im Gerät eingebauten WLAN-Chip zur Erkennung und Verbindung mit dem Netzwerk.

Universitäten mussten seit jeher dafür sorgen, eine ausgewogene Balance zwischen Benutzerfreundlichkeit und Sicherheit zu schaffen. Es ist wichtig, den sicheren Zugang nicht mühsam zu machen – sonst finden Studenten und andere Benutzer eine Umgehung oder verwenden „Schatten-IT-Geräte“. Beispielsweise benötigen Gäste in manchen Campusnetzwerken einen „Sponsor“, um sich am Netzwerk authentifizieren zu können. In anderen werden Gäste zu einem Self-Service-Portal geleitet, wo sie Informationen zu ihrer Person eingeben und der Verwendung eines angemessenen Sprachgebrauchs zustimmen müssen, bevor sie sich anmelden können. Beide Verfahren bieten den gleichen Schutz für das Netzwerk, das eine ist jedoch etwas lästiger als das andere.

8 https://www.vmware.com

In einer Defense-in-Depth-Architektur zählt Netzwerkzugriffssicherheit zu den wichtigsten Investitionen überhaupt. Auf dieser Ebene liegt die Zuständigkeit für die „4 A“: Authentifizierung, Autorisierung, Audit und Administration. Eine erfolgreiche Authentifizierung führt zur Autorisierung des Zugriffs auf die Netzwerkressourcen, die für eine bestimmte Rolle freigegeben sind. Audit umfasst die Überwachung des Netzwerkverkehrs und -verhaltens. Bei anormalen Verhaltensmustern verhängt die Administration Quarantäne oder setzt Regeln für den Netzwerkdatenverkehr um.

Die „4 A“ werden unter anderem durch folgende Technologien für Netzwerkzugriffssicherheit unterstützt:

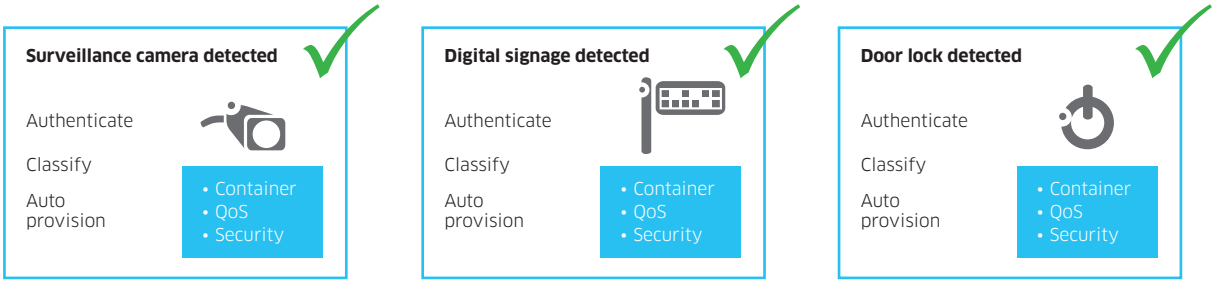
1. 802.1X: Ein portbasiertes Network-Access-Control-Verfahren (NAC) nach IEEE-Standard, das einen Authentifizierungsmechanismus für LAN- und WLAN-Geräte bereitstellt. 802.1X erfordert einen Supplicant (Computer oder Gerät, das Zugriff anfordert), einen Authenticator (normalerweise der Ethernet-Switch, WLAN AP oder Controller) sowie einen Authentication Server (in der Regel ein RADIUS- oder EAP-Server). Der Supplicant übermittelt die Anmeldeinformationen an den Authentication Server. Wenn diese gültig sind, gewährt der Authenticator Zugriff auf das Netzwerk.
2. Biometrie: Eine neue, potenziell benutzerfreundlichere Sicherheitsauthentifizierungsmethode ist die Nutzung biometrischer Daten oder anderer einzigartiger Benutzermerkmale, z. B. Fingerabdruck, Iris-Scan oder Sprachprofil. Dies ist eine einfache und sichere Methode, einem Menschen Zugriff auf das Netzwerk zu gewähren – bei IoT-Geräten hilft dieses Verfahren jedoch leider nicht weiter.
3. Verschlüsselung: Während sie früher als Sicherheitsmechanismus für Daten bei der Speicherung und während der Übertragung von einem Rechenzentrum zum anderen verwendet wurde, kommt die MACSec-Verschlüsselung inzwischen vor allem im LAN zum Einsatz – vom Systemkern bis zur Netzwerkgrenze. Darüber hinaus ist die Verschlüsselung auch in den IEEE WLAN-Standards definiert, nämlich in Form des Standards 802.11i, der WLAN-Übertragungen vom Access Point zum Benutzer vor Man-in-the-Middle-Angriffen schützen soll (einer der wichtigsten Gründe, kein öffentliches, unverschlüsseltes WLAN zu verwenden). Zudem hat die Wi-Fi Alliance kürzlich den neuen Standard WPA3 (Wi-Fi Protected Access 3) angekündigt. Die neuen Funktionen von WPA3 vereinfachen die WLAN-Sicherheit, ermöglichen robuste Authentifizierung und bieten stärkere Verschlüsselungsgrade für besonders sicherheitsempfindliche Datenmärkte, während sie aber zugleich die Ausfallsicherheit für geschäftskritische Netze wahren.
4. Gehärtetes Betriebssystem: Viele Netzwerkgeräte werden mit standardmäßigen Administrator-Authentifizierungsprofilen geliefert. Leider – und bei IoT-Geräten fast immer – werden diese Standards nicht geändert, wodurch das Gerät eine leichte Beute für das Einschleusen von Malware oder gar Manipulationen am Code wird. Ein gehärtetes Gerätebetriebssystem chiffriert den Code und Speicherort, sodass ein erfolgreicher Angriff auf ein Gerät nicht automatisch erfolgreich wiederholt werden kann. Neben dem verbesserten Schutz der Integrität des Geräts kann ein gehärtetes Betriebssystem auch folgende Merkmale aufweisen:
    1) Erkennen und Entschärfen von DoS-Angriffen: Manche Netzwerkinfrastrukturgeräte können einen DoS-Angriff erkennen und sofort vereiteln, indem der betreffende Datenverkehr unterbunden wird.
    2) Erkennen von IP-basierten Angriffen: Manche Netzwerkinfrastrukturgeräte sind in der Lage, SNORT oder andere IDS/IDP-Produkte einzubinden. Dadurch können sie auf eine positive IPAngriffssignatur reagieren und den betreffenden Datenverkehr in Quarantäne schicken.
5. Unified Network Access Policies (UNAP): Nach erfolgreicher Authentifizierung autorisiert diese Regelstruktur den Netzwerkzugriff anhand von Parametern wie MAC-Adresse, Tageszeit, Benutzerrolle, Abteilung (z. B. Studierende, Gäste, Fakultät, Mitarbeiter, Lieferanten, Verwaltung, Zulassungen, Sport) oder sogar dem Standort, an dem die Authentifizierung erfolgt. Die Struktur, die sowohl LAN- als auch WLAN-Zugriff unterstützt, verhindert die Falschzuordnung oder Duplizierung von Sicherheitsprofilen und ermöglicht einen konsistenten, sicheren Netzwerkzugriff.
6. IoT-Geräte: Unified Network Access Policies sind eine wichtige Voraussetzung für die Unterstützung von IoT-Geräten. Darüber hinaus können mithilfe von DHCP Device Fingerprinting IoT-Geräte verschiedener Hersteller schnell identifiziert werden. Diese Funktion nutzt DHCP-Optionen zur Bereitstellung von herstellerspezifischen Informationen über die Gerätehardware oder das Betriebssystem. Der Informationsaustausch mithilfe der DHCP-Optionen erfolgt gemäß der Definition in RFC 2132.[9] Die durch die DHCP-Optionen bereitgestellten Anbieter-, Geräte- und Betriebssysteminformationen bilden in ihrer Gesamtheit den „Fingerabdruck“ des Geräts. Beispiel: Eine Ausschreibung für Überwachungskameras (CCTV) wurde an einen einzelnen Hersteller vergeben. Die neuen Produkte werden in Koexistenz mit den alten CCTV-Kameras verwendet.

9 http://www.ietf.org/rfc/ rfc2132.txt

Dank der Implementierung von UNAP verfügt das Team über zwei Möglichkeiten zur Identifizierung und Anwendung von Netzwerksicherheitsregeln: DHCP Fingerprinting oder MAC-Adressenmaskierung. Bei der MAC-Adressenmaskierung werden nur die ersten 24 Bit der MAC-Adresse genutzt, die den Organizationally Unique Identifier (OUI) enthalten[10]. Durch die Anwendung von UNAP mit einer maskierten MAC-Adresse kann die Institution ihre neuen Überwachungskameras schnell und sicher in den Betrieb einbinden. Und DHCP Fingerprinting ermöglicht es der Campus-IT, alle Überwachungskameras zu identifizieren und konsistente Sicherheitsrichtlinien durchzusetzen.

DHCP Device Fingerprinting wird normalerweise von WLAN-Systemen unterstützt, hat aber seine Stärken insbesondere dann, wenn auch LAN-Geräte vorhanden sind, da nicht alle IoT-Geräte über WLAN mit dem Netzwerk verbunden sind.

Abbildung 2. Automatische Erkennung und Klassifizierung

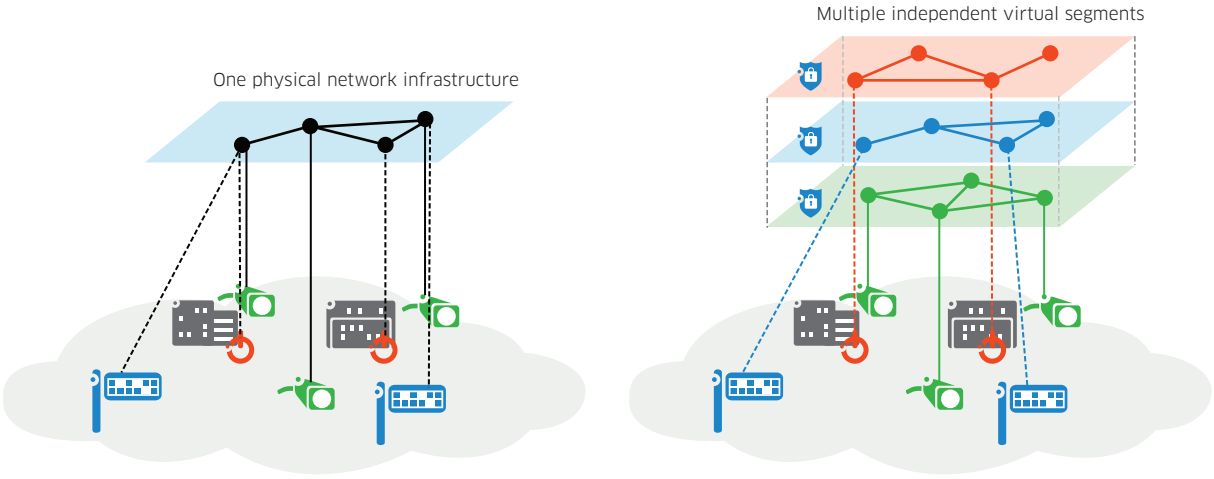


Netzwerksegmentierung

Mit der Einführung von LAN-Switching wurde die Netzwerksegmentierung über die physische Segmentierung hinaus auch auf virtuelle LANs (VLANs) ausgeweitet. Dadurch können Netzwerkservices für Benutzer, die Mitglieder des VLAN sind, eingeschränkt werden, um Anwendungen und Dienste abzusichern. Die meisten Netzwerkgeräte unterstützen bis zu 4.096 VLANs. Dies scheint mehr als genug zu sein, doch in der Realität stellt dies eine Herausforderung dar und erfordert eine saubere Strukturierung.

Die VLAN-Ressourcenerschöpfung ist ein reales Problem, für das diverse Technologien entwickelt wurden, die von Hochschulen eingesetzt werden. MPLS (Multiprotocol Label Switching)[11] und das davon abgeleitete Shortest Path Bridging (SPB – IEEE 802.1aq[12]) nutzen beide das Konzept von Serviceschnittstellen zur weiteren Segmentierung der Netzwerkaktivitäten.

Abbildung 3. SPBM – Netzwerksegmentierung, ohne Spanning Tree



10 http://standards-oui.ieee.org/oui/oui.txt
11 https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
12 https://en.wikipedia.org/wiki/IEEE_802.1aq

Netzwerkmanagement

Netzwerkmanagement ist eine häufig übersehene Anwendung von Infrastruktur-Anbietern. Dafür gibt es viele Gründe. Der wichtigste ist die verbreitete Nutzung von Drittanbieter-Anwendungen, die auch die Verwaltung von Multivendor-Umgebungen ermöglichen. Die Verwendung eines Drittanbieter-Netzwerkmanagementsystems (NMS) bringt jedoch auch Nachteile mit sich. Viele herstellereigene NMS-Plattformen berücksichtigen vorhandene Supportberechtigungen und empfehlen sogar Wartungs-Releases, die mögliche Fehler in der Implementierung beheben. Darüber hinaus bieten OEM-NMS in der Regel eine Fülle von Statistiken, Analysen und Trenddiagrammen, die ein proaktives Netzwerkmanagement ermöglichen.

Inzwischen richten IT-Experten in Bildungseinrichtungen den Blick auch verstärkt auf Deep Packet Inspection-Funktionalitäten (DPI) für die LAN-Infrastruktur. Die Information, welche Anwendungen die meiste Bandbreite verbrauchen, ist wichtig für die gesamte IT-Abteilung, um zu wissen, an welchen Stellen Investitionen erforderlich sind. Wenn zum Beispiel der Datenverkehr von und zu der LMSAnwendung der größte Bandbreitenverbraucher ist, empfiehlt es sich wahrscheinlich, die der LMS VM zugewiesenen Ressourcen zu prüfen. Und bei einer cloudbasierten Implementierung lässt sich durch eine Analyse der Benutzererfahrung bestimmen, ob zusätzliche Investitionen zur Erhöhung der Bandbreite, Arbeitsspeicher- bzw. Prozessorgeschwindigkeit oder Speicherkapazität nötig sind.

Für die Cybersicherheit auf dem Campus ist das NMS die zentrale Steuerungsplattform. Von der Aktivierung von SSL-verschlüsseltem CLI-Zugriff auf die Infrastrukturkomponenten bis zur Implementierung von Unified Network Access Policies, Überwachung des Datenverkehrs auf Anomalien oder Isolierung von verhaltensauffälligen Geräten oder Benutzern in Quarantäne – das NMS ist die Plattform zur Durchführung all dieser und weiterer Aufgaben.

Zusätzlich zu einem leistungsstarken NMS sollten einige Drittanbieter-Anwendungen in Erwägung gezogen werden:

1. perfSONAR[13]: Dieses Tool wird von vielen Forschungseinrichtungen verwendet und bietet Funktionen, die einen Überblick über die gesamte Netzwerkleistung geben. Hier eine Kurzbeschreibung zum Zweck dieses Tools:

   „Es ist wichtig, sicherzustellen, dass alles durchgängig optimal funktioniert. Die allgemein übliche und akzeptierte Praxis ist die Überwachung einer einzelnen Domäne, da eine domänenübergreifende Leistungsüberwachung mit herkömmlichen Tools schwer zu realisieren ist. perfSONAR ist eine vielfach genutzte Test- und Messinfrastruktur, die von Wissenschaftsnetzwerken und Instituten auf der ganzen Welt zur Überwachung und Sicherstellung der Netzwerkleistung eingesetzt wird."
2. Zusätzliche Fehlerbehebungstools in perfSONAR:
   1) pScheduler: Durchsatztests zu externen Standorten
   2) OWAMP: Laufende Überprüfung auf Latenz und Paketverlust

Zusammenfassung

Bildungseinrichtungen stellen weltweit die dritthäufigsten Ziele für Cyberangriffe dar. Cybersicherheit im Bildungswesen ist kein Luxus, sondern eine kritische Dimension in der Systemarchitektur, und kann zu einem positiven Image einer Universität beitragen.

Durch Einführung einer risikobasierten Sicherheitsplanung wird es der Universität ermöglicht, Budgetmittel auf Basis des Bedarfs oder Risikos zu verteilen. Eine Defense-in-Depth-Architektur gewährleistet, dass ein Angreifer erst unterschiedliche Technologien überwinden muss, bevor er erfolgreich sein kann.

Die Klassifizierung Ihrer Cyberressourcen anhand der CIA-Triade Vertraulichkeit, Integrität und Verfügbarkeit hilft Ihnen, die Risiken für Ihre Institution zu ermitteln und zu priorisieren.

Die Implementierung der „4 A" (Authentifizierung, Autorisierung, Audit und Administration) schafft eine einheitliche Struktur für den Netzwerkzugriff und das Netzwerkverhalten in LAN- und WLANNetzwerken.

13 https://www.perfsonar.net/about/what-is-perfsonar/

Darüber hinaus ermöglicht die Segmentierung des Netzwerks mit MPLS oder SPB eine granulare Steuerung der Services sowie der Geräte und Benutzer, die auf diese Services zugreifen.

Und schlussendlich das Thema Schulung: Sicherheitstechnologien und -architekturen leisten einen großen Beitrag zum Schutz Ihrer Systeme. Wie schon vielen Studien nachgewiesen haben, sind jedoch Phishing und Benutzerfehler die häufigsten Ursachen für Sicherheitsverletzungen. Durch intensive Schulung von Studierenden, Dozenten, Mitarbeitern und Lieferanten zu Themen Cybersicherheit können Sie diesen Risikofaktor Nummer 1 reduzieren.

Referenzen und Ressourcen

National Institute of Standards and Technology: Über diesen Link gelangen Sie auf die Seite des Cybersicherheits-Frameworks NIST: https://www.nist.gov/cyberframework

EDUCAUSE: Eine gemeinnützige Vereinigung, die Hochschulen beim optimalen Einsatz von IT unterstützt. Die Ergebnisse der jährlichen Umfrage „Top 10 IT Issues" für 2018 sowie Links zu weiteren Ressourcen finden Sie hier: https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education

Alcatel·Lucent Enterprise