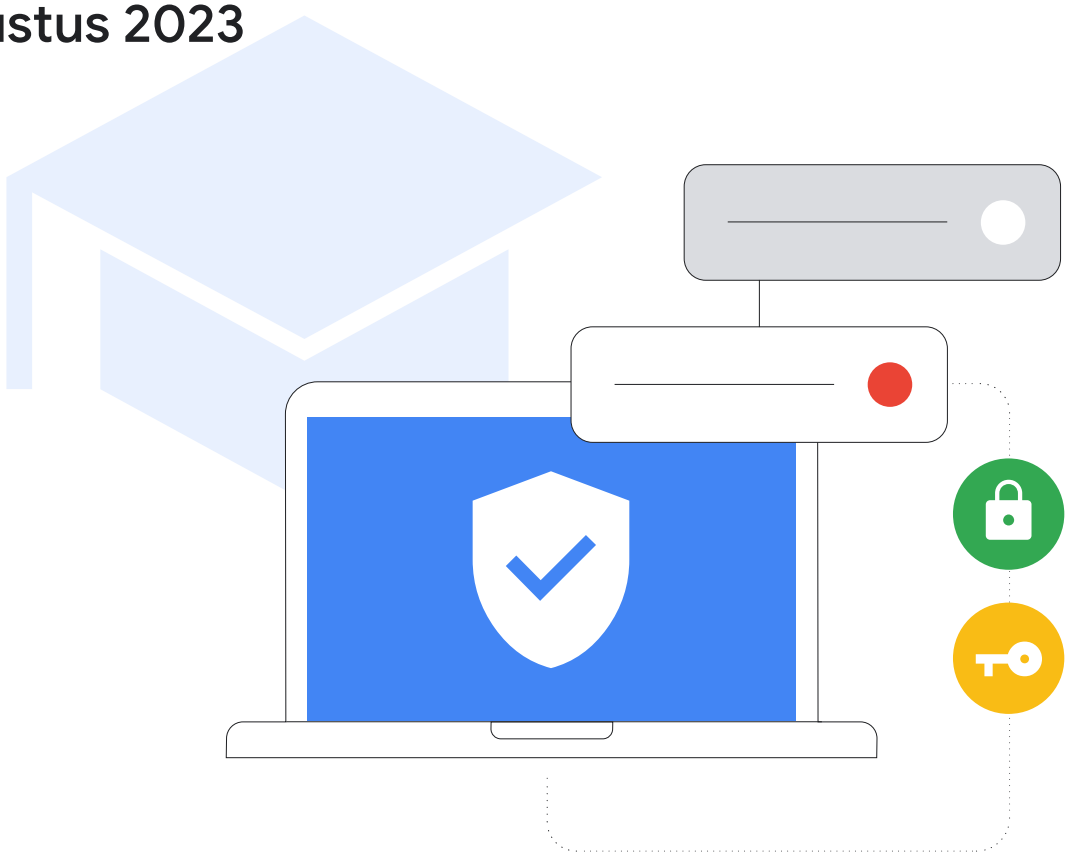
Google for Education

Buku Panduan Pengamanan Siber di Sekolah Dasar dan Menegah

Diperbarui Agustus 2023



Safer with Google

Ringkasan Eksekutif

Seperti ditegaskan dalam laporan Protecting Our Future CISA, institusi sekolah dasar dan menengah perlu berinvestasi dalam pengamanan siber untuk melindungi siswa, keluarga, pengajar, staf, dan komunitas mereka. Dokumen ini memberikan panduan dan praktik terbaik bagi admin IT sekolah dalam menyiapkan serta mengonfigurasi hardware dan software di institusi sekolah dasar dan menengah untuk memperkuat pengamanan siber mereka. Di dalamnya tercakup praktik terbaik umum serta panduan spesifik untuk berbagai produk dan layanan Google. Misi Google untuk mengelola informasi dunia serta membuatnya berguna dan dapat diakses semua orang menjadi pendorong penting bagi upaya kami di tim Google for Education dalam membuat alat yang dirancang untuk pengajaran dan pembelajaran. Kami akan menyampaikan pelajaran dari upaya tersebut dalam panduan ini.

Kami menyajikan praktik terbaik keamanan berdasarkan topik untuk memberikan pemahaman lebih mendalam tentang konfigurasi, penyiapan, dan strategi mitigasi risiko. Kami juga menjelaskan pendekatan Google terhadap pengamanan siber untuk aneka layanan kami, khususnya alat untuk pendidikan. Meskipun panduan mendetail dalam dokumen ini disajikan tanpa memandang produk atau layanannya, kami yakin produk kami menawarkan perlindungan terbaik dari berbagai serangan umum sejak pertama kali dijalankan.

Risiko

Institusi pendidikan merupakan target utama serangan siber. Pihak-pihak yang tidak bertanggung jawab terus berupaya mengeksploitasi lingkungan sekolah yang kaya akan data untuk keuntungan mereka sendiri. 46% sekolah yang sejauh ini "selamat" yakin bahwa pada akhirnya mereka pun akan menjadi sasaran mengingat semakin canggihnya, dan semakin sulit dihentikannya, serangan ransomware. Dan 42% sekolah tersebut merasa bahwa ransomware sedemikian lazimnya sehingga serangannya tidak terelakkan. Kebutuhan sekolah untuk segera beralih ke model pembelajaran jarak jauh pada tahun 2020 menjadi pemicu utama terciptanya celah pengamanan siber, yang membuat sebagian sekolah rentan terhadap serangan.

Pertahanan

Serangan tersebut dapat dimitigasi. Dan meskipun tidak ada teknologi yang mampu menghilangkan risiko tersebut sepenuhnya, sektor pendidikan dan vendor teknologi pendidikan dapat bekerja sama untuk mengadopsi dan menerapkan praktik terbaik guna menciptakan pendekatan yang aman, terlindung, serta komprehensif untuk mengurangi risiko secara signifikan. Dengan menerapkan langkah pencegahan serta kebijakan yang tepat untuk melindungi pengguna, mengamankan perangkat, dan memastikan privasi data, institusi pendidikan dapat mengelola risiko dan memitigasi serangan dengan lebih baik.

Rekomendasi Utama:

- **GUNAKAN AUTENTIKASI YANG AMAN** untuk menjaga keamanan informasi sensitif, melindungi email, file, serta konten lainnya, dan mencegah pengguna yang tidak berwenang mengakses sistem pendidikan. Gunakan praktik terbaik untuk autentikasi pengguna, termasuk sandi yang kuat dan verifikasi dua langkah (2SV), kunci sandi, serta pengelola sandi jika memungkinkan, khususnya bagi admin IT dan staf yang menangani informasi sensitif.
- **TERAPKAN SETELAN KEAMANAN YANG TEPAT** untuk menjaga keamanan pengguna, data, dan lingkungan Anda. Meskipun produk-produk Google didesain agar aman secara default, admin tetap harus memanfaatkan serta mengonfigurasi jaringan dan sistem dengan tepat untuk memastikan keamanan. Untuk menjaga agar sekolah tetap aman, terapkan prinsip *zero-trust* dan hak istimewa terendah. Artinya, akses pengguna ke software, data, aplikasi, dan sistem harus dibatasi hanya sejauh yang diperlukan untuk menjalankan pekerjaan mereka secara efektif.
- **UPDATE DAN UPGRADE SISTEM** untuk memastikan pengguna terlindung dari ancaman terbaru. Gunakan sistem operasi (OS) dan browser yang modern, serta pastikan pengguna menjalankan versi software terbaru di semua perangkat (atau versi stabil jangka panjang yang disetujui) dan mengaktifkan update otomatis. Melakukan upgrade ke solusi yang lebih aman, seperti Chromebook, dapat meningkatkan keamanan. Belum pernah ada serangan ransomware yang terdeteksi di perangkat ChromeOS apa pun.
- **GUNAKAN SISTEM PEMBERITAHUAN DAN PEMANTAUAN REAL-TIME** untuk meningkatkan postur keamanan dan memitigasi potensi masalah dengan cepat. Anda dapat menggunakan fitur yang terintegrasi dalam software kolaborasi dan komunikasi utama Anda, seperti Google Workspace for Education, atau mengimplementasikan solusi *logging* dan pemantauan keamanan terpisah. Pastikan pelacakan aktivitas yang komprehensif di seluruh jaringan, perangkat, aplikasi, pengguna, dan data sekolah Anda. Pantau login akun, pembagian file, volume email (terutama upaya phishing dan malware), aktivitas perangkat, dan perubahan konfigurasi. Selalu perbarui solusi pemberitahuan dan pemantauan Anda untuk menerima notifikasi tentang ancaman, peristiwa penting, dan perubahan sistem.
- **BERIKAN PELATIHAN KEPADA PENGAJAR, STAF, DAN SISWA** tentang cara aman menggunakan perangkat dan software, mengenali dan melaporkan potensi ancaman, serta berbagi data dengan tepat untuk membantu melindungi institusi dari beberapa jenis serangan yang paling umum. Sekolah atau dinas pendidikan dapat membuat materi pelatihan sendiri, serta menggunakan materi siap pakai yang tersedia gratis, untuk menyusun toolkit yang komprehensif bagi sekolah.

[1] https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Rekomendasi khusus bagi pengguna produk Google:

Produk Google, seperti Google Workspace for Education dan Chromebook, dapat meningkatkan pengamanan siber di sekolah Anda dan memudahkan penerapan setiap rekomendasi di atas. Jika digunakan bersama-sama, produk tersebut akan memberikan solusi komprehensif yang membantu melindungi privasi pengguna dan menghadirkan keamanan terbaik di kelasnya untuk institusi Anda.

Semua strategi di atas, beserta panduan tambahan yang diberikan dalam dokumen ini, akan membentuk fondasi yang kokoh bagi keamanan institusi sekolah dasar dan menengah.

Pendekatan Google terhadap Pendidikan

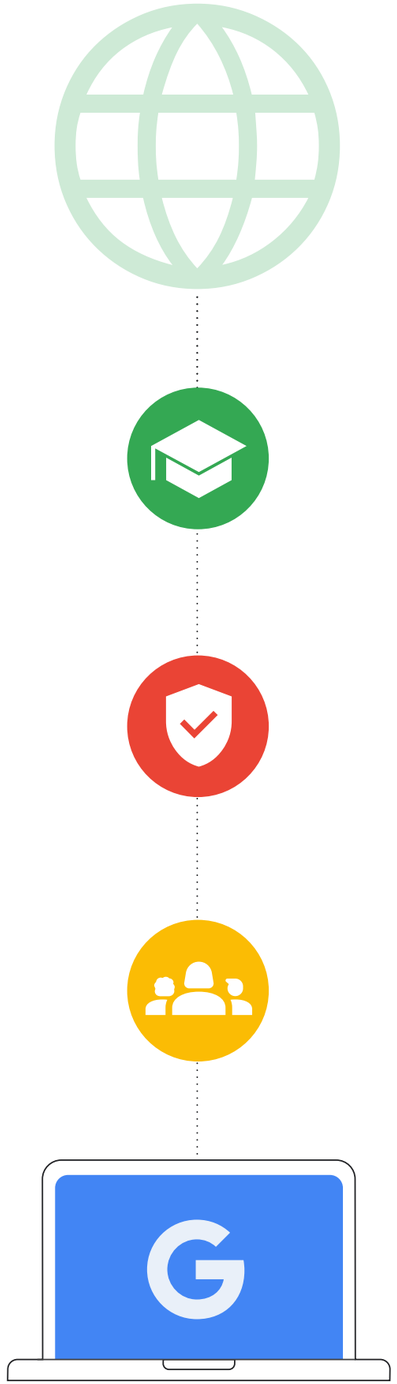
Misi Google untuk mengelola informasi dunia serta membuatnya berguna dan dapat diakses semua orang sangat relevan dengan sektor pendidikan. Di tim Google for Education, kami mengemban misi tersebut dengan menciptakan alat seperti Chromebook dan Google Classroom yang memungkinkan pengajar dan siswa membuat, membagikan, dan mengelola konten, juga mengakses dan menggunakan referensi pendidikan serta alat online, dengan mudah dan aman.

Sekolah pantas mendapatkan teknologi yang aman secara default, didesain dengan mempertimbangkan privasi, menempatkan Anda sebagai pengendali, serta memiliki konten dan informasi yang tepercaya. Dengan produk seperti Chromebook dan Google Workspace for Education, sekolah mendapatkan keamanan terbaik di kelasnya yang mematuhi standar pendidikan global tertinggi, admin IT memiliki visibilitas menyeluruh dan kontrol yang mudah atas kebijakan data dan keamanan sekolah, sementara siswa dapat menikmati sepenuhnya proses pembelajaran di lingkungan digital yang lebih aman, menyajikan konten sesuai usia, serta memitigasi spam dan ancaman siber.

Kami memiliki fitur dan kontrol keamanan bawaan yang diprioritaskan, standar privasi tertinggi, dan opsi alat keamanan yang lebih proaktif untuk memastikan lingkungan pembelajaran yang aman bagi siapa saja. Perangkat ChromeOS membantu memitigasi ancaman yang mengintai sekolah, dan merupakan pertahanan terbaik dari ancaman nomor satu mereka—ransomware—karena belum pernah ada serangan ransomware yang berhasil terhadap Chromebook.

Sementara itu, Google Workspace for Education adalah salah satu paket aplikasi komunikasi dan kolaborasi berbasis cloud paling aman dan populer di dunia. Untuk informasi selengkapnya tentang bagaimana setiap produk melindungi pengamanan siber dalam kaitannya dengan rekomendasi yang disajikan dalam dokumen ini, silakan baca bagian terakhir.

Dokumen ini terbagi atas dua bagian. Bagian pertama berisi panduan keamanan umum dan praktis bagi institusi sekolah dasar dan menengah terlepas dari produk yang digunakan. Bagian kedua menyajikan panduan konfigurasi spesifik bagi institusi yang menggunakan produk Google for Education seperti Google Workspace for Education dan Chromebook. Kedua bagian tersebut akan memberikan informasi untuk membantu Anda dan siswa Anda tetap aman saat beraktivitas online.



Pengantar

Perangkat dan jaringan institusi sekolah dasar dan menengah berisiko tinggi menjadi target serangan siber. Oleh karena itu, institusi sekolah dasar dan menengah harus menerapkan pengamanan sebaik mungkin untuk melindungi siswa dan mencegah hilangnya data, layanan, sumber daya, waktu, dan anggaran yang dapat ditimbulkan oleh serangan tersebut. (Sumber)

Panduan ini adalah alat untuk mempromosikan praktik terbaik pengamanan siber yang dapat diterapkan administrator sekolah dan sistem sekolah untuk mengamankan lingkungan mereka dengan lebih baik. Dengan menerapkan praktik terbaik ini, institusi sekolah dasar dan menengah akan dapat memitigasi atau mencegah serangan cyber yang serius dan sangat merugikan terhadap sistem pendidikan serta melindungi siswa, keluarga, pengajar, dan staf.

Serangan siber yang menarget sekolah makin meningkat frekuensi dan keparahannya. Menurut K-12 Cybersecurity Resource Center, ada lebih dari 1.300 insiden cyber yang diungkapkan kepada publik yang melibatkan organisasi pendidikan di 50 negara bagian Amerika Serikat antara tahun 2016 dan 2021. Para pemimpin institusi pendidikan saat ini harus melindungi data dan informasi pribadi siswa, pengajar, dan staf, serta sistem dan informasi institusi mereka. Ini adalah tugas yang berat, terutama karena sektor pendidikan secara tradisional lebih sulit mengimbangi langkah pengamanan siber dibandingkan dengan sektor lain.

Serangan siber yang berhasil, termasuk ransomware, phishing, malware, dan lainnya, dapat berujung pembobolan data informasi identitas pribadi (PII) berskala besar, biaya yang mahal (rata-rata pembayaran tebusan meningkat 5x lipat sejak tahun 2020 menjadi $812.260), dan gangguan berkepanjangan terhadap pengajaran dan operasi lain di sekolah. Baru-baru ini, sebuah serangan ransomware yang berhasil telah melumpuhkan seluruh sistem sekolah dan menimbulkan efek berantai di seluruh komunitas karena siswa tidak dapat bersekolah selama berhari-hari. Dengan sumber daya dan dana yang terbatas, organisasi sekolah dasar dan menengah akan terus menjadi target utama, kecuali jika mereka meningkatkan investasi dalam pengamanan siber.

Cara terbaik untuk menghadirkan pengamanan siber adalah melalui komunikasi, kolaborasi, dan kemitraan. Dokumen ini dikompilasi dari tips keamanan dan keselamatan Google, Kerangka Kerja Pengamanan Cyber National Institute for Standards and Technology (NIST), serta Toolkit dan Rekomendasi dari 2023 CISA K-12 Cybersecurity sebagai sumber praktik pengamanan siber yang diterima secara luas. Dokumen ini membahas langkah-langkah umum yang perlu diambil atau dipertimbangkan oleh admin TI, beberapa praktik terbaik dan panduan Google untuk produk-produk kami, serta menyertakan referensi ke berbagai tips dan layanan keamanan yang ditawarkan perusahaan lain. Sebaiknya administrator mempelajari semua panduan keamanan dari perusahaan yang relevan dan menerapkan panduan terbaru mereka, karena perusahaan yang bertanggung jawab adalah perusahaan yang mampu menjelaskan produknya sendiri beserta semua perubahan yang mungkin telah terjadi.

Sebelum mengambil tindakan atas rekomendasi yang tercantum di bawah, sebaiknya Anda juga mempertimbangkan faktor-faktor berikut:

Pertimbangan:

1. **Melindungi populasi siswa.**
   Kebutuhan setiap sekolah berbeda-beda, dan populasi tertentu mungkin memerlukan langkah tambahan untuk melindungi keamanan dan privasi. Banyak alat teknologi pendidikan memiliki fitur yang dapat memudahkan penerapan akses berbasis usia, seperti membatasi konten tidak pantas atau memastikan kerahasiaan data lokasi dan kontak mereka.
2. **Jenis data yang disimpan.**
   Jika menyimpan data sensitif, sebaiknya Anda mengenkripsi data tersebut atau menyimpannya di lokasi terpisah.
3. **Jenis perangkat yang digunakan dan model implementasi.**
   Perangkat dan aplikasi yang berjalan di perangkat tersebut harus mendapatkan update otomatis untuk memaksimalkan keamanan, mengenkripsi data, dan mengisolasi akun untuk memastikan pengguna hanya memiliki akses ke informasi mereka sendiri.
4. **Kebijakan sekolah, dinas pendidikan kabupaten/kota dan provinsi.**
   Sekolah Anda mungkin menerapkan kebijakan spesifik terkait penggunaan teknologi. Anda perlu memastikan bahwa semua pengamanan disiapkan sesuai dengan kebijakan tersebut.

Setiap hari
100 juta
upaya phishing diblokir oleh Gmail.

Setiap minggu
300,000
situs tidak aman diidentifikasi oleh Google.

Setiap hari
74 juta
pengguna mendapatkan bantuan dari Pengelola Sandi Google.

Setiap tahun
700 juta
orang memperkuat keamanan mereka dengan Pemeriksaan Keamanan.

Menggunakan Autentikasi yang Aman

Autentikasi yang aman harus menjadi prioritas utama sekolah dan institusi lainnya. Pada kuartal keempat tahun 2022, akun yang lemah atau tanpa kredensial menyumbang 48% dari semua faktor penyusupan dalam pembobolan data. Menerapkan beberapa rekomendasi utama dapat membantu memverifikasi keaslian identitas pengguna dan membatasi akses ke informasi yang sesuai dengan peran setiap pengguna.

Admin IT harus menerapkan verifikasi dua langkah (2SV, disebut juga autentikasi 2 langkah (2FA)), dan beralih ke metode autentikasi tanpa sandi (yaitu, kunci sandi) jika memungkinkan, dan terutama setiap kali seseorang mengakses sistem institusi pendidikan dari jarak jauh. Verifikasi 2 Langkah menambahkan lapisan keamanan ekstra ke akun online Anda sehingga mempersulit penyerang mendapatkan akses.

Ada banyak jenis perangkat dan model implementasi yang digunakan sekolah saat ini, dan kemampuan teknis di lingkungan sekolah dasar dan menengah berbeda-beda. Pengamanan akun dan perangkat yang berlaku untuk berbagai peran dan jenis pengguna juga bervariasi, dengan praktik terbaik: admin TI, pengajar dan staf, serta siswa yang lebih senior menggunakan perangkat individual, sementara siswa yang lebih junior menggunakan perangkat bersama. Kami akan membahas rekomendasi spesifik untuk setiap kelompok di bawah.

Ada beberapa jenis metode autentikasi yang merupakan praktik terbaik dalam sebagian besar situasi:

- **Sandi yang kuat**
  Minta pengguna untuk membuat sandi mereka sendiri ketika pertama kali login dan secara teknis wajibkan kerumitan dan panjang minimum sandi. Frasa sandi yang lebih panjang memberikan elemen keamanan tambahan karena lebih panjang dan menggunakan karakter yang kompleks. Sebaiknya pengguna tidak sering-sering diminta mengubah sandi karena hal itu akan mendorong mereka untuk menggunakan sandi yang lebih sederhana atau membuat perubahan yang tidak signifikan (seperti mengubah satu karakter).
- **Verifikasi dua langkah (2SV)**
  Verifikasi 2 Langkah melindungi akun dengan langkah kedua—sering kali sesuatu yang dimiliki pengguna, seperti kunci keamanan atau aplikasi di ponsel yang menghasilkan kode verifikasi sekali pakai. Meskipun semua bentuk Verifikasi 2 Langkah meningkatkan keamanan akun, sebaiknya administrator menghindari penggunaan kode verifikasi yang dikirim melalui SMS atau telepon yang bisa jadi rentan terhadap serangan berbasis nomor telepon.
- **Autentikasi tanpa sandi**
  Kunci sandi merupakan alternatif sandi yang lebih aman dan lebih mudah. Pengguna dapat login ke aplikasi dan situs dengan PIN, pola, sensor biometrik (seperti sidik jari atau pengenalan wajah), atau ketukan kunci keamanan, sehingga mereka tidak perlu mengingat dan mengelola sandi. Meskipun mungkin tidak cocok untuk setiap lingkungan pendidikan, metode ini makin menggeser penggunaan autentikasi tradisional serta membuat proses login jadi lebih cepat dan lebih aman. Kunci sandi melindungi pengguna dari serangan phishing karena hanya dapat digunakan di situs dan aplikasi yang telah mereka daftarkan.
- **Single Sign-On (SSO)**
  SSO memungkinkan pengguna mengakses banyak aplikasi dan situs dengan satu set kredensial. Karena hanya perlu mengingat satu set kredensial, kemungkinan pengguna untuk menuliskannya menjadi lebih kecil. Selain itu, jika tidak perlu mengelola banyak set kredensial pengguna, sekolah dapat menghemat biaya dukungan dan layanan bantuan IT. Google Workspace for Education mendukung SSO secara *native* sehingga pengguna dapat menggunakan kredensial Akun Google mereka untuk login ke aplikasi pihak ketiga, atau menggunakan kredensial penyedia lain untuk login ke Akun Google mereka.
- **Pengelola sandi**
  Pengelola sandi dapat membantu pengguna membuat sandi yang kuat dan unik di seluruh akun dan layanan yang mereka gunakan selama hari sekolah dan hari kerja (jika tidak menggunakan SSO). Pengelola sandi tidak membantu login ke sistem operasi perangkat, tetapi dapat mengelola sandi setelah pengguna login. Pengguna Google dapat menggunakan Pengelola Sandi di Chrome pada semua platform, termasuk ChromeOS dan Android.

Subset atau kombinasi khusus dari beberapa pendekatan autentikasi di atas akan berguna bagi bermacam grup yang memiliki kebutuhan unik, sesuai dengan peran mereka di institusi pendidikan, jenis sistem dan data yang dapat mereka akses, serta usia mereka.

Administrator Sekolah

Di institusi sekolah dasar dan menengah, administrator mengontrol sistem dan sebagian besar data. Perlindungan akun mereka menjadi kunci keamanan seluruh sistem: mulai dari infrastruktur, data akun, hingga perangkat yang dikelola institusi. Oleh karena itu, mereka harus mengadopsi standar autentikasi terbaik, termasuk menggunakan sandi yang kuat, pengelola sandi yang andal, dan Verifikasi 2 Langkah. Setiap metode tersebut memberikan lapisan perlindungan yang, jika digunakan bersama-sama, akan memberikan keamanan terkuat bagi akun Administrator dan layanan institusi.

- Administrator harus menggunakan kunci keamanan fisik atau metode 2SV yang aman dari segi kriptografi, yang memerlukan perangkat tepercaya dan dialog. Ini dapat berupa layanan seperti Google Authenticator atau aplikasi lain yang menghasilkan kode verifikasi sekali pakai. Chromebooks yang dirilis setelah tahun 2019 dengan chip TPM memiliki tombol daya yang dapat digunakan untuk autentikasi 2 langkah.
- Administrator harus menggunakan pengelola sandi tepercaya yang mendukung Verifikasi 2 Langkah untuk menyimpan sandi ke berbagai layanan.

Siswa lebih senior (biasanya kelas 4 ke atas) yang menggunakan perangkat individual

Siswa yang lebih senior lebih memahami cara melindungi diri mereka sendiri dan biasanya mampu menggunakan mekanisme autentikasi yang lebih protektif, yang sesuai dengan jenis layanan yang kemungkinan mereka gunakan. Sebaiknya mereka hanya diberi akses ke akun mereka sendiri dan informasi yang telah dibagikan kepada mereka..

- Siswa yang menggunakan Chromebook perlu diberi opsi untuk membuat PIN spesifik per perangkat guna mempercepat proses login di perangkat tersebut. Opsi biometrik mungkin tidak sesuai atau tidak memungkinkan untuk diterapkan di banyak lingkungan sekolah.
- Setiap siswa harus didukung dalam membuat sandi unik yang tidak menyertakan informasi pribadi (misalnya nama, kelas, atau tanggal lahir). Siswa perlu diberi tahu bahwa frasa sandi dapat memberikan sandi yang cukup kompleks sekaligus mudah diingat.

Pengajar dan staf yang menggunakan perangkat individual

Seperti halnya administrator, pengajar dan staf memiliki akses ke data sensitif, tetapi mereka tidak mengontrol infrastruktur digital dan memiliki kemampuan teknis yang lebih beragam.

- Pengajar dan staf yang menggunakan Chromebook sebaiknya diberi opsi untuk login dengan verifikasi biometrik, seperti sidik jari, jika hal itu diizinkan secara hukum.
- Administrator perlu menerapkan Verifikasi 2 Langkah dan beralih ke metode autentikasi tanpa sandi jika memungkinkan dan setiap kali anggota staf mengakses sistem institusi pendidikan dari jarak jauh.

Siswa lebih junior (biasanya kelas 3 ke bawah) yang menggunakan perangkat bersama

Siswa yang paling junior masih belajar cara menggunakan teknologi pendidikan, dan autentikasi sederhana—yang sesuai untuk digunakan dengan layanan dan data terbatas—akan lebih memudahkan mereka.

- Sekolah yang menggunakan metode pengganti sandi dari pihak ketiga, seperti kode QR atau login dengan gambar, untuk siswa yang paling junior dan yang tidak dapat login dengan sandi, sebaiknya menerapkan tindakan pencegahan demi keamanan karena metode tersebut kurang aman. Administrator perlu mengubah sandi siswa dan memperbarui kode setiap kali kode hilang atau diketahui orang lain.
- Sekolah harus mengedukasi siswa dan orang tua tentang pentingnya menjaga kerahasiaan sandi dan menyimpan kredensial alternatif seperti kode QR dengan aman.
- Untuk perangkat individual seperti tablet, PIN spesifik per perangkat dapat digunakan sebagai metode autentikasi alternatif yang aman.

Menerapkan Setelan Keamanan yang Sesuai

Perangkat dan jaringan sekolah adalah target dengan visibilitas dan nilai yang tinggi bagi penyerang di seluruh dunia. Oleh karena itu, gunakan keamanan terbaik untuk mencegah hilangnya layanan, sumber daya, waktu, dan anggaran. Administrator sistem harus menerapkan fitur keamanan yang efektif dan sesuai, yang tersedia dalam produk yang digunakan institusi mereka. Mereka juga perlu memastikan bahwa sistem tersebut tetap mudah digunakan oleh pengajar, staf, dan siswa. Setelan keamanan dan privasi penting harus dikonfigurasi sedemikian rupa sehingga tidak dapat dinonaktifkan atau diubah oleh setiap pengguna, dan setelan lainnya harus dilindungi dengan nilai default yang ditetapkan oleh administrator. Gunakan keamanan terbaik untuk mencegah hilangnya layanan, sumber daya, waktu, dan anggaran. Jika menggunakan Chromebook, Anda dapat melihat saran kami tentang cara menyetel kebijakan perangkat di bagian akhir dokumen ini.

Terakhir, integrasikan "minimalisasi data" ke dalam praktik Anda dengan membatasi tujuan dan sarana pengumpulan, penggunaan, dan pengungkapan informasi pribadi individu sesuai kebutuhan yang wajar dan proporsional untuk menyediakan layanan atau yang sejalan dengan konteks hubungan.

Aplikasi & Update

Batasi dan minimalkan aplikasi yang dapat diinstal pengguna karena setiap aplikasi yang diinstal di perangkat berpotensi menjadi vektor serangan yang dapat dieksploitasi. Jika memungkinkan, gunakan aplikasi dari sumber tepercaya. Misalnya, anjurkan pengguna memeriksa keberadaan badge verifikasi di Google Play Store untuk memastikan bahwa mereka mendownload aplikasi resmi yang telah ditinjau keamanannya. Segala modifikasi OS atau hardware (melalui *jailbreak* atau *rooting*) akan memasukkan cacat keamanan yang signifikan dan harus dihindari.

Akses & Visibilitas

Administrator harus memastikan pengguna hanya dapat mengakses data, software, layanan, dan sistem yang diperlukan untuk menjalankan pekerjaan mereka secara efektif. Hal ini akan membantu membatasi akses yang tidak diinginkan dan melacak siapa yang memiliki akses ke sumber daya tertentu. Berikan perhatian khusus terhadap data sangat sensitif, seperti PII pengguna, dan sistem (seperti HR, penggajian, penilaian, keamanan, dan konfigurasi) dengan mengaudit pengguna mana yang dapat mengakses data tersebut dan dalam keadaan apa, dengan membatasi akses ke perangkat milik sekolah, serta memastikan akses hanya dimiliki oleh anggota staf tertentu.

Tinjau kebijakan berbagi data institusi Anda di alat kolaborasi untuk mencegah praktik berbagi yang tidak tepat atau terlalu luas dan akses tanpa izin. Batasi atau blokir pembagian data dengan pihak di luar institusi Anda (terutama oleh siswa) dan terapkan kebijakan untuk memantau pembagian konten sensitif.

Kehilangan atau Pencurian Perangkat

Kehilangan perangkat tidak harus berarti kehilangan data. Administrator perlu membakukan rencana untuk memastikan akses ke informasi dan dokumen sebagai jaga-jaga jika perangkat hilang atau dicuri, misalnya dengan mengelola dokumen di lingkungan cloud. Download dan cetak kode cadangan untuk proses Verifikasi 2 Langkah guna mencegah gangguan akses akun.

Jika perangkat dilaporkan hilang atau dicuri, pastikan perangkat tersebut dikunci dari jarak jauh jika memungkinkan, dan akun yang terkait juga dikunci atau ditandai untuk memastikan akun tersebut tidak digunakan untuk memperoleh akses tanpa izin. Chromebook dapat dihapus total dari jarak jauh jika hilang, dan akun Google Workspace for Education dapat dipantau untuk mendeteksi aktivitas yang mencurigakan, atau bahkan ditangguhkan (dikunci) jika perlu.

Perlindungan Lanjutan bagi Pengguna Berisiko Tinggi

Untuk pengguna yang memiliki peran penting dan informasi sensitif (termasuk admin Google Workspace for Education), Google menyediakan Program Perlindungan Lanjutan (APP). APP memberikan perlindungan tambahan dari serangan tertarget, seperti upaya phishing, download berbahaya, dan pembobolan sandi. APP didesain secara khusus untuk menggagalkan serangan online tertarget atas Akun Google, dan otomatis menggunakan autentikasi yang kuat, kunci keamanan, serta membatasi akses pihak ketiga ke data akun. Penyedia akun online lainnya juga menawarkan perlindungan akun yang kuat bagi pengguna berisiko tinggi, yang sebaiknya selalu digunakan oleh admin dan staf yang memiliki akses ke informasi pribadi atau sistem teknologi.

Mengupdate dan Mengupgrade Sistem

Salah satu upaya terpenting yang dapat dilakukan setiap orang untuk melindungi dirinya sendiri adalah selalu mengupdate sistem operasi dan aplikasi di perangkat miliknya. Hal ini menjadi makin penting bagi institusi sekolah dasar dan menengah, mengingat peran vital mereka dalam pendidikan dan kehidupan sehari-hari anak. Sebagian besar serangan malware, baik di lingkungan pendidikan maupun lingkungan berisiko tinggi lainnya, menarget perangkat berbasis Windows, termasuk SolarWinds, serangan ransomware terhadap Los Angeles Unified School District, peretasan Little Rock School District, pembobolan data Microsoft Exchange Server, serangan ransomware terhadap Albuquerque School District, dan yang terbaru pembobolan data di agensi federal Microsoft. Lingkungan sekolah adalah tempat lainnya di mana penggunaan produk dan layanan cloud akan mempermudah tugas administrator dengan mengurangi permukaan serangan serta memastikan sistem dan aplikasi selalu diupdate secara otomatis.

Melakukan Upgrade ke Sistem Operasi Modern dan Selalu Mengupdatenya

Versi terbaru setiap sistem operasi (OS) biasanya berisi fitur keamanan baru untuk membantu mencegah vektor serangan yang diketahui. Sebaiknya Anda mengaktifkan fungsi update otomatis di dalam OS perangkat, atau jika update otomatis tidak dimungkinkan, download dan instal patch serta update dari vendor tepercaya setidaknya sebulan sekali.

Chromebook menjalankan ChromeOS sehingga sering menerima update otomatis yang berisi patch keamanan terbaru untuk mempercepat penerapan inovasi keamanan terbaru dan memverifikasi integritas sistem operasi hanya-baca sebelum dilakukan booting. Chromebook juga mengenkripsi semua data yang tersimpan di perangkat sehingga terlindung dari akses tanpa izin. Selain itu, setiap halaman web dan aplikasi dijalankan di sandbox terpisah sehingga infeksi malware pada satu situs atau aplikasi tidak akan menyebar ke bagian lain di perangkat yang sama.

Jika sekolah Anda belum siap untuk beralih ke Chromebook, ChromeOS Flex adalah versi ChromeOS yang dibuat untuk memodernisasi perangkat sekolah. ChromeOS Flex memberi semua orang pengalaman pengajaran dan pembelajaran yang modern dan terpadu, serta memiliki keamanan bawaan yang proaktif dan kemampuan pengelolaan berbasis cloud. Flex dapat memberikan perlindungan otomatis serta memblokir file yang dapat dieksekusi dan aplikasi berbahaya tanpa mengharuskan Anda untuk mengganti hardware yang sudah ada.

Melakukan Upgrade ke Browser Modern dan Selalu Mengupdatenya

Pastikan browser juga diupdate dan aman. Browser modern menawarkan fitur keamanan lebih canggih yang dapat diaktifkan dengan mudah oleh pengguna atau dikonfigurasi oleh administrator agar aktif secara default di komputer institusi. Dengan begitu, fitur tersebut akan membantu melindungi kerahasiaan informasi sensitif saat dikirim melalui Internet. Browser harus selalu diupdate. Baik saat bekerja, belajar, maupun melakukan aktivitas online lainnya, browser modern yang terupdate akan:

- **Menerapkan pengamanan yang andal,** termasuk isolasi situs dan perlindungan safe browsing untuk mencegah pengguna membuka situs berbahaya secara tidak sengaja
- **Mengaktifkan update otomatis** untuk memastikan browser mendapatkan update keamanan dengan cepat.
- **Memastikan keamanan koneksi** Browser modern menggunakan Transport Layer Security, dan pengguna dapat mengklik di sebelah URL untuk memeriksa apakah koneksi ditandai sebagai aman atau tidak

Chrome dibuat dengan mempertimbangkan keamanan, dengan fitur keamanan seperti safe browsing yang aktif secara default. Ada juga pengelola sandi terintegrasi yang dapat mengisi sandi secara otomatis saat Anda menjelajah web, sehingga Anda dapat menggunakan sandi yang kuat dengan mudah.

Menggunakan Sistem Pemberitahuan dan Pemantauan Real-Time

Sistem pemberitahuan dan pemantauan real-time dapat membantu sekolah mengidentifikasi dan merespons ancaman dengan cepat sebelum menyebabkan kerusakan. Pastikan alat keamanan berjalan di latar belakang agar dapat mengumpulkan dan mencatat peristiwa keamanan dari seluruh sistem. Alat AI sangat bagus dalam menyaring data yang terkumpul dalam jumlah besar serta menemukan anomali dan pola, yang dapat digunakan untuk mendeteksi ancaman dengan lebih cepat dan mudah, juga memproses dan mengatasi kerentanan. Hal ini memungkinkan pemrioritasan aktivitas yang perlu ditinjau oleh staf atau admin IT.

Sekolah dapat menggunakan fitur pemberitahuan dan pemantauan yang disertakan dalam software kolaborasi dan komunikasi utama mereka, seperti Google Workspace for Education, atau mengimplementasikan solusi Security Information and Event Management (SIEM) terpisah.

Sistem pemberitahuan dan pemantauan real-time dapat melacak berbagai aktivitas di jaringan, perangkat, aplikasi, pengguna, dan data sekolah, seperti login pengguna, akses ke file, potensi pembobolan, percobaan pencurian data atau pencurian data yang berhasil, dan aktivitas administrator.

Jika mendeteksi aktivitas yang mencurigakan, sistem dapat mengirimkan pemberitahuan kepada staf IT sekolah. Dengan begitu, admin dapat menginvestigasi masalahnya dan mengambil tindakan untuk memitigasi ancaman tersebut.

Selain itu, alat pemberitahuan dan pemantauan dapat digunakan untuk memperoleh pemahaman lebih mendalam tentang ancaman yang dihadapi sekolah. Dengan menganalisis data dari sistem real-time ini, sekolah dapat mengidentifikasi tren dan pola yang dapat membantu mereka meningkatkan perlindungan.

Berikut ini beberapa praktik terbaik terkait penggunaan sistem pemberitahuan dan pemantauan (termasuk SIEM):

1. **Menetapkan sasaran keamanan**
   Identifikasi informasi dan sistem yang paling penting bagi sekolah serta jenis ancaman yang memunculkan risiko terbesar terhadap informasi dan sistem tersebut. Selanjutnya, identifikasi data yang perlu dikumpulkan untuk memantau kemunculan ancaman itu.
2. **Mengumpulkan data yang tepat & mengonfigurasi aplikasi dengan benar**
   Kumpulkan data yang tepat dan konfigurasi aplikasi guna mencapai sasaran keamanan Anda yang paling relevan. Data yang dikumpulkan dapat mencakup data dari firewall, filter konten, Intrusion Detection System, server web, dan perangkat keamanan lainnya, beserta software komunikasi dan kolaborasi, Sistem Informasi Sekolah, dan Sistem Pengelolaan Pembelajaran.
3. **Menginvestigasi dan merespons pemberitahuan**
   Saat sistem pemantauan Anda memunculkan pemberitahuan, investigasi masalah itu dan ambil tindakan yang tepat. Tindakan ini dapat mencakup menyatukan berbagai tim untuk menyelidiki sumber pemberitahuan, menentukan apakah pemberitahuan tersebut positif palsu (PP) atau bukan, atau mengambil langkah untuk memitigasi ancaman, seperti menangguhkan akun, mereset sandi pengguna, mengarantina atau menghapus email, mengubah izin file, atau menghapus total perangkat.

Melatih Pengajar, Staf, dan Siswa

Institusi sekolah dasar dan menengah harus meningkatkan kesadaran dan kebiasaan keamanan komunitas sekolah, dengan sosialisasi dan kemitraan untuk memberdayakan pengguna mereka. Mengedukasi pengajar, staf, dan siswa tentang pentingnya keamanan sangat diperlukan untuk membantu mereka melindungi diri secara online dan membantu mencegah ancaman keamanan siber yang serius. Ajari mereka cara menggunakan produk dan layanan yang ada di seluruh institusi, cara menemukan dan melaporkan ancaman seperti email phishing, dan yang paling penting, cara mengambil tindakan untuk mencegah serangan tersebut. Sekolah dan dinas pendidikan perlu meningkatkan kesadaran dan kebiasaan keamanan komunitas sekolah, dengan sosialisasi dan kemitraan untuk memberdayakan pengguna mereka.

Cara Aman Menggunakan Perangkat dan Software

Administrator dapat bermitra dengan pengajar dan pakar dalam mengembangkan kurikulum pengamanan siber di tingkat yang sesuai usia untuk membantu siswa memahami cara menggunakan perangkat, software, dan sistem dengan aman. Materi pelatihan buatan sekolah atau dinas pendidikan dapat membantu memberikan konteks terhadap rekomendasi yang diberikan kepada pengajar dan siswa. Anda juga dapat memanfaatkan materi siap pakai yang tersedia, seperti Tangkas Berinternet yang tersedia di Safety.Google dan Khan Academy, lalu menyesuaikannya dengan kebutuhan Anda. Program-program tersebut dapat membantu pengguna untuk tetap aman di mana pun mereka berada, baik di sekolah maupun di komunitas mereka.

Mengenali Ancaman

Melatih pengajar, staf, dan siswa untuk mengenali ancaman merupakan bagian penting dalam upaya menjaga keamanan mereka. Mengajari anak-anak cara mengetahui apakah sesuatu termasuk ancaman atau bukan merupakan hal yang penting, karena mereka mungkin tidak tahu cara membedakan mana yang sah dan mana yang tidak. Ada beberapa jenis ancaman yang harus mereka kenali dan pahami cara melaporkannya, dan administrator harus berfokus pada topik-topik yang menurut mereka akan memberikan dampak paling signifikan. Yang penting, pelatihan sebaiknya tidak hanya mengajari pengguna cara mengenali ancaman, tetapi juga mengambil tindakan. Ancaman umum yang perlu dikenali pengguna mencakup ransomware, phishing, manipulasi psikologis, malware, dan penipuan. Namun, jika ancaman tertentu lebih sering terjadi di institusi tertentu, pastikan komunitas sekolah diedukasi mengenai hal itu.

Praktik Berbagi Data dan File yang Aman

Pengajar dan staf harus dilatih tentang cara berbagi data dan file yang tepat, serta cara mengenali permintaan yang tidak pantas melalui email. Yang terpenting, mereka harus memastikan bahwa informasi pribadi sensitif hanya dibagikan atau diproses jika diperlukan dan dengan lapisan perlindungan tambahan, misalnya dengan tidak membagikan data semacam itu melalui email atau kepada pihak eksternal. Mereka harus menggunakan kemampuan pencegahan kebocoran data (disertakan dengan ChromeOS dan Workspace for Education) untuk memperingatkan dan mencegah pengguna akhir berbagi file yang mengandung data sensitif (seperti nomor jaminan sosial) atau menyalin dan menempel konten sensitif di luar domain..

Penerapan Pendekatan Google: Perangkat dan Layanan untuk Pendidikan

Pengadaan software adalah salah satu metode paling ampuh bagi dinas pendidikan untuk melindungi diri. Software harus dirancang dan dibangun dengan arsitektur yang kuat untuk meminimalkan risiko kerentanan, dengan keamanan yang terintegrasi di setiap lapisannya. Dengan mewajibkan sekolah membeli software yang aman, atau software dari perusahaan dengan rekam jejak keamanan yang terbukti, risiko siber yang lebih luas dapat dikurangi secara signifikan. Sebagai contoh, di Google, kami mempertangguh keamanan ChromeOS sambil terus men gimplementasikan solusi yang lebih proaktif dan cerdas yang memanfaatkan keunggulan kami dalam machine learning, cloud, dan teknologi identitas.

Google berkomitmen untuk menciptakan produk yang membantu melindungi privasi siswa dan pengajar serta memberikan jaminan keamanan terbaik bagi institusi Anda. Anda tidak perlu ragu bahwa produk dan layanan Google for Education terus melindungi pengguna, perangkat, dan data dari ancaman yang makin kompleks. Bagian ini akan memandu admin IT sekolah menerapkan rekomendasi keamanan ketika menggunakan produk-produk Google for Education.

Google Workspace for Education

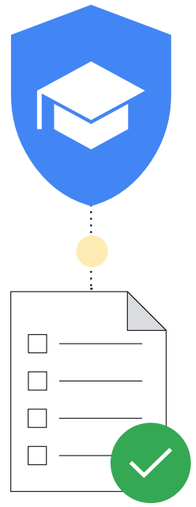
Google Workspace for Education adalah serangkaian alat dan layanan Google yang disesuaikan untuk sekolah agar dapat berkolaborasi, mengefisienkan proses pengajaran, serta menjaga pembelajaran tetap aman. Produk dan layanan Google for Education melindungi pengguna, perangkat, dan data secara terus-menerus dari ancaman yang makin kompleks, serta menyediakan alat seperti pusat notifikasi dan keamanan, vault untuk eDiscovery, Pengelolaan Akses dan Identitas, serta pencegahan kebocoran data.

Bagi Anda yang baru mulai menggunakan Google Workspace for Education, kami telah menghimpun berbagai materi berguna, yang banyak di antaranya dapat membantu Anda menyiapkan segala sesuatunya sesuai dengan rekomendasi yang diberikan dalam panduan ini. Untuk bantuan tentang cara memulai Google Workspace for Education, lihat Panduan memulai cepat penyiapan TI.

Checklist Keamanan

Tinjau checklist keamanan untuk mempelajari lebih lanjut cara memperkuat keamanan dan privasi institusi Anda. Sekolah yang menggunakan Google Workspace for Education edisi Standard dan Plus juga dapat menggunakan halaman Kondisi Keamanan untuk memantau konfigurasi setelan konsol Admin. Misalnya, Anda dapat memeriksa status setelan seperti penerusan email otomatis, enkripsi perangkat, setelan berbagi Drive, dan lain-lain. Jika diperlukan, Anda dapat menyesuaikan setelan domain berdasarkan pedoman dan praktik terbaik keamanan umum, sembari menyeimbangkan pedoman tersebut dengan kebutuhan bisnis dan kebijakan manajemen risiko organisasi Anda.

Alasan sektor pendidikan diperkirakan akan terkena serangan



Sumber: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Berikut ini beberapa tips berguna lainnya untuk memastikan Anda memaksimalkan perlindungan bawaan Google Workspace for Education:

Menyiapkan Unit Organisasi (OU)

Semua orang sepakat bahwa setiap pengguna di akun Google Workspace for Education Anda perlu menggunakan setelan yang sama. Unit organisasi adalah grup-grup pengguna yang memungkinkan Anda memberikan layanan, setelan, dan izin yang berbeda kepada pengguna yang berbeda, misalnya menggunakan Verifikasi 2 Langkah bagi pengajar dan staf, dan autentikasi sesuai usia untuk siswa yang lebih junior. Siapkan unit organisasi untuk staf, untuk pengajar, dan untuk siswa guna menerapkan kebijakan ke setiap grup pengguna secara terpisah. Struktur yang dirancang dengan baik sangat penting untuk mengelola akun Google Workspace for Education Anda secara efektif dan fleksibel.

Menyiapkan Kebijakan Sandi dan Perlindungan Akun Admin

Seperti yang telah kita bahas, autentikasi pengguna merupakan bagian penting dalam upaya menjaga keamanan institusi Anda. Karena itulah, kami telah menyiapkan cara fleksibel bagi Administrator untuk mengelola autentikasi, yang akan memungkinkan Anda memastikan bahwa pengguna memiliki perlindungan akun yang tepat dan aman. Tetapkan kebijakan sandi untuk memastikan bahwa pengguna membuat sandi yang kuat, dan pertimbangkan untuk mewajibkan penggunaan Verifikasi 2 Langkah, jika memungkinkan, berdasarkan pengelompokan yang direkomendasikan di bagian Login Aman. Anda dapat menerapkan Verifikasi 2 Langkah untuk sekumpulan pengguna (dengan memberi mereka waktu untuk menyiapkannya) dan mengimplementasikan Verifikasi 2 Langkah melalui berbagai metode, termasuk kunci keamanan (paling aman), dialog Google (menggunakan aplikasi Google di Android dan iOS), pembuat aplikasi verifikasi (seperti Google Authenticator), dan pesan teks atau panggilan telepon (meskipun paling tidak aman).

Jika organisasi Anda menggunakan Penyedia Identitas (IdP) selain Google, Anda dapat menyiapkan Single Sign On (SSO) melalui Penyedia Identitas pihak ketiga. Anda tetap dapat menggunakan Verifikasi 2 Langkah bersama SSO untuk akun selain admin super, jika diinginkan.

Mengaktifkan atau Menonaktifkan Layanan

Administrator dapat mengontrol layanan Google mana saja yang dapat diakses pengguna dengan akun Google Workspace for Education mereka dari konsol Google Admin. Anda dapat mengontrol akses ke layanan Google seperti Kalender, Drive, dan Meet dengan mengaktifkan atau menonaktifkan layanan berdasarkan unit organisasi (OU) (Anda juga dapat mengaktifkan layanan saat menggunakan grup). Anda juga dapat meninjau perbedaan antara layanan Inti dan Tambahan Workspace sebelum mengaktifkan layanan tambahan seperti YouTube, Google Maps, dan Blogger. Administrator dianjurkan untuk menetapkan akses ke layanan Google berdasarkan usia. Ingat, pengguna yang ditetapkan sebagai berusia di bawah 18 tahun akan otomatis dikenai pembatasan di beberapa layanan Google saat login ke akun Google Workspace for Education mereka.

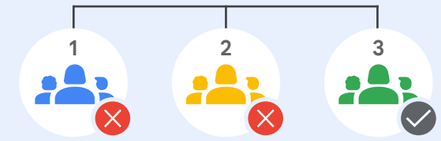
Anda juga dapat menggunakan Akses Kontekstual (tersedia di Workspace for Education Standard dan Plus) untuk mengizinkan atau memblokir akses ke aplikasi Google seperti Gmail, Drive, dan Kalender berdasarkan alamat IP, asal geografis, kebijakan keamanan, atau OS perangkat. Misalnya, Anda dapat mengizinkan Drive untuk desktop hanya di perangkat milik perusahaan di negara/wilayah tertentu.

Metode untuk memberi pengguna akses ke layanan

Di konsol Google Admin, Anda dapat menonaktifkan akses unit organisasi ke layanan Google, seperti Google Drive. Jika beberapa pengguna di unit organisasi tersebut perlu menggunakan Drive, Anda memiliki 2 opsi:

1. Pindahkan pengguna ke unit organisasi yang mengaktifkan Drive.
2. Tambahkan pengguna pada grup akses, lalu aktifkan Drive untuk grup. Setiap anggota dapat mengakses layanan, meskipun unit organisasinya menonaktifkan layanan tersebut.

Unit organisasi



Google Drive dinonaktifkan untuk unit organisasi 1 dan 2.

Di dalam grup akses

Namun, **grup pengguna** di unit organisasi 1 dan 2 dapat mengakses Google Drive

Sumber: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Menetapkan Kebijakan Berbagi Data dan Aturan Retensi

Sebagai administrator, Anda dapat mengontrol apakah pengguna dapat membagikan file dan folder Google Drive kepada orang di luar organisasi. Langkah ini dapat membantu mencegah praktik berbagi data dan file yang tidak diinginkan atau terlalu luas, sehingga akan mencegah terjadinya kebocoran data. Pemisahan file dan drive, pembuatan unit organisasi, dan pengoperasian sesuai prinsip hak istimewa terendah merupakan langkah penting untuk mencegah penyerang berpindah-pindah di jaringan jika mereka berhasil menyusup ke satu akun. Makin terbatas akses data dan jaringan yang dimiliki calon penyerang, makin kecil kerusakan yang dapat ditimbulkan.

Nonaktifkan fitur berbagi file eksternal untuk siswa (atau batasi aktivitas berbagi eksternal hanya ke domain yang diizinkan) dan tetapkan "Pemeriksa akses" ke "Hanya penerima". Jika Anda mengizinkan sebagian atau semua pengguna untuk berbagi file ke luar domain, aktifkan peringatan saat pengguna melakukannya. Selain itu, nonaktifkan publikasi file di web, dan wajibkan kolaborator eksternal untuk login dengan Akun Google.

Pelanggan Workspace for Education Standard dan Plus juga dapat menggunakan Target Audiens dan Aturan Kepercayaan untuk menetapkan rekomendasi dan pembatasan berbagi secara lebih terperinci. Misalnya, dengan Target Audiens, Anda dapat menetapkan audiens berbagi link default untuk pengajar ke "pengajar dan staf", bukan semua orang di institusi Anda. Dengan Aturan Kepercayaan, Anda dapat memblokir siswa sekolah dasar sehingga tidak dapat membagikan file kepada siswa yang lebih senior.

Tinjau kebijakan drive bersama untuk memastikan bahwa hanya pengguna yang tepat yang dapat membuat drive bersama, dan mencegah pengguna eksternal mengakses drive bersama. Sebaiknya Anda hanya mengizinkan admin (atau staf dan pengajar) untuk membuat drive bersama dan mengelola akses ke drive bersama dengan cermat.

Pertimbangkan untuk membatasi visibilitas Direktori dan berbagi kontak jika mungkin, baik dengan menonaktifkan berbagi kontak untuk sebagian atau semua pengguna, maupun dengan membuat direktori kustom untuk membatasi pengguna mana yang terlihat oleh pihak lain tertentu.

Siapkan kebijakan pencegahan kebocoran data (DLP) di Drive dan Gmail untuk mendeteksi dan memblokir informasi sensitif. Beberapa kebijakan standar dapat dimanfaatkan untuk melindungi informasi sensitif yang umum (seperti nomor rekening bank atau kartu kredit). Anda juga dapat membuat kebijakan kustom berdasarkan kata kunci, daftar kata, dan ekspresi reguler (Regex).

Mengelola Setelan Gmail

Gmail adalah salah satu layanan inti dalam Google Workspace for Education, dan ada banyak setelan yang dapat dimanfaatkan administrator untuk melindungi institusi dan pengguna mereka.

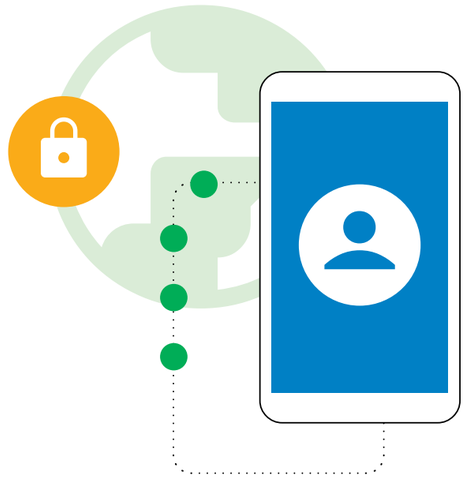
Cegah spam, spoofing, dan phishing dengan autentikasi Gmail. Sesuaikan setelan filter spam, termasuk mewajibkan autentikasi pengirim untuk semua pengirim yang disetujui dan menonaktifkan opsi pengabaian filter spam untuk pengirim internal.

Nonaktifkan akses POP/IMAP jika memungkinkan, dan aktifkan pemindaian yang dipertajam untuk pesan sebelum dikirim serta perlindungan lanjutan terhadap phishing dan malware. Jika Anda mengizinkan email eksternal untuk sebagian atau semua pengguna, Anda dapat mengaktifkan peringatan penerima eksternal.

Pelanggan Google Workspace for Education Standard dan Plus juga dapat membantu melindungi institusi dari serangan malware dan ransomware dengan menyiapkan aturan untuk mendeteksi lampiran berbahaya menggunakan Sandbox Keamanan.

Aplikasi Pihak Ketiga

Gunakan alur kerja persetujuan bawaan untuk menyetujui aplikasi pihak ketiga yang mengakses data akun melalui API. Langkah ini membantu mencegah pembagian data tanpa izin kepada aplikasi pihak ketiga yang tidak disetujui untuk penggunaan di lingkungan sekolah.



Laporan dan Pemantauan

Sebagai administrator, Anda dapat melihat laporan dan peristiwa log di konsol Google Admin untuk meninjau aktivitas di organisasi Anda seperti potensi risiko keamanan, melihat siapa yang login dan kapan, serta memahami cara pengguna membuat dan membagikan konten. Anda dapat melihat data tingkat domain beserta detail tingkat pengguna yang terperinci melalui grafik dan tabel. Lihat laporan dan log audit (termasuk pusat notifikasi) untuk mengidentifikasi risiko keamanan, menganalisis penggunaan layanan, mendiagnosis masalah konfigurasi, melacak aktivitas pengguna, dan banyak lagi.

Administrator Google Workspace for Education Standard dan Plus dapat memanfaatkan Dasbor Keamanan untuk melihat ringkasan berbagai laporan keamanan, mengidentifikasi tren, dan membandingkan data saat ini dengan data historis, seperti aktivitas berbagi file di Drive, spam, phishing, dan malware di Gmail, login akun pengguna yang mencurigakan, dan aktivitas perangkat yang mencurigakan. Sebagian besar log penggunaan, aktivitas, dan audit—termasuk peristiwa log Admin, Drive, Meet, dan Chat—serta laporan keamanan, tersedia selama enam bulan.

Memanfaatkan Pusat Keamanan

Administrator Google Workspace for Education Plus dan Standard dapat memanfaatkan pusat keamanan, yang menyediakan informasi dan analisis keamanan lanjutan, serta visibilitas dan kontrol yang lebih baik mengenai masalah keamanan yang memengaruhi domain.

Pusat keamanan mencakup Alat Investigasi Keamanan, yang dapat membantu administrator mengidentifikasi, memprioritaskan, dan mengambil tindakan terhadap masalah keamanan dan privasi, seperti serangan phishing, pembagian file yang tidak tepat, aktivitas pengguna dan perangkat yang mencurigakan, serta masih banyak lagi.

Google Workspace adalah rangkaian alat komunikasi dan kolaborasi berbasis cloud paling aman di dunia

0

kerentanan software yang dieksploitasi secara aktif di Workspace sejak November 2021*

50%

potensi penghematan premi asuransi pengamanan siber dengan menggunakan Workspace

2x lebih sedikit

insiden keamanan di organisasi yang menggunakan Workspace vs Microsoft 365

2.5x lebih sedikit

insiden keamanan di organisasi yang menggunakan Workspace vs. Microsoft Exchange

*Menurut CISA, jumlah ini jauh lebih sedikit daripada vendor produktivitas lainnya di pasar ini.

Google Chromebook untuk Pendidikan

Chromebook adalah komputer untuk siswa dan pengajar yang sangat aman, skalabel, dan mudah digunakan berkat fitur keamanan bawaan yang langsung aktif sejak pertama dijalankan. Belum pernah ada laporan serangan ransomware terhadap perangkat ChromeOS apa pun, baik yang digunakan di lingkungan bisnis, sekolah, maupun konsumen. Chromebook membantu melindungi sekolah dari ancaman yang terus berkembang dengan fitur-fitur terupdate. Update berlangsung secara otomatis di latar belakang sehingga pengguna dapat kembali bekerja dalam hitungan detik.

Update OS dan aplikasi secara otomatis, dengan perlindungan malware bawaan

Penyerang terus berusaha memanfaatkan bug dan celah dalam sistem operasi, browser, serta aplikasi populer untuk menginstal malware dan mencuri data pengguna. Untuk melindungi Anda dan pengguna, Chromebook selalu mengupdate OS dan aplikasi Anda karena perangkat ini didesain aman secara default dengan update keamanan, dan aplikasi cloud tidak membutuhkan update software seperti halnya aplikasi lokal. Chip keamanan rancangan Google di Chromebook membantu menjaga keamanan perangkat, melindungi identitas pengguna, dan memastikan integritas sistem.

Chromebook di inventaris perangkat Anda akan menjalankan update perlindungan malware terbaru secara otomatis. Siswa dan pendidik terlindung dari ancaman siber dengan fitur keamanan bawaan seperti enkripsi data, booting terverifikasi, sandboxing, dan update otomatis.

Data pengguna yang aman

Saat Anda login ke Chromebook dengan Akun Google, semua data Anda disimpan sebagai file terenkripsi, sehingga tidak ada orang lain di perangkat tersebut yang dapat melihat data Anda atau login ke aplikasi menggunakan akun Anda. Hal ini membuat siswa dapat berbagi perangkat dengan sangat mudah dan aman di kelas, dan sekolah dapat mengurangi total biaya komputasi. Untuk menikmati fitur keamanan yang lebih canggih, lisensi pengelolaan perangkat yang disebut Chrome Education Upgrade menawarkan peningkatan visibilitas.

Kebijakan keamanan perangkat terkelola untuk pengguna jarak jauh

Administrator sekolah dapat mengonfigurasi kebijakan ChromeOS dan menginstal/mengupdate aplikasi dari jarak jauh menggunakan konsol Google Admin. Dengan sekali mengklik tombol, seorang admin IT dapat memperbarui kebijakan dan konfigurasi di ratusan ribu Chromebook dalam sekejap.

Hal ini memastikan bahwa

- Siswa hanya dapat mengakses konten dan aplikasi yang disetujui oleh sekolah
- Semua aplikasi dan ekstensi diupdate dengan perbaikan keamanan terbaru
- Pengguna tidak dapat menyalin, mentransfer, atau membagikan data sekolah di luar perangkat
- Keputusan berbasis data dapat diambil dengan rekomendasi keamanan yang disesuaikan dari Google untuk mengatasi ancaman keamanan
- Kebijakan keamanan serta pengelolaan akses dan identitas dapat dikelola secara terpusat untuk semua pengguna, langsung dari konsol Admin

Beberapa kebijakan penting yang mungkin perlu dikonfigurasi administrator adalah:

Kebijakan Perangkat

- **Mode Tamu**
  Sebaiknya nonaktifkan mode Tamu di perangkat sekolah sehingga siswa dan pengajar harus login menggunakan kredensial mereka, bukan menggunakan perangkat secara anonim.
- **Pembatasan login**
  Anda mungkin tidak ingin siswa dan pengajar login ke Chromebook sekolah menggunakan akun Gmail pribadi mereka. Terapkan pembatasan agar login dibatasi hanya ke domain Workspace sekolah untuk perangkat yang digunakan secara eksklusif oleh siswa.
- **Pelaporan pengguna dan perangkat**
  Admin sebaiknya mempertimbangkan untuk mengaktifkan pelaporan pengguna dan perangkat sehingga mereka dapat mengumpulkan metrik terkait seberapa sering Chromebook digunakan, siapa yang menggunakan, dan bagaimana kondisi hardware Chromebook tersebut.
- **Pendaftaran ulang paksa**
  Chromebook milik sekolah harus tetap berada di sekolah, kecuali jika administrator mencabut aksesnya. Sebaiknya admin mempertimbangkan untuk mengaktifkan pendaftaran ulang paksa Chromebook sehingga Chromebook akan selalu mendaftar ulang secara otomatis jika ada upaya untuk menghapus total atau mencurinya.

Kebijakan Pengguna

- **Mode Samaran**
  Chromebook sekolah harus disiapkan agar siswa dapat menggunakannya tanpa gangguan. Hal ini termasuk membatasi siswa agar hanya dapat mengakses browser terautentikasi, sehingga filter konten web dapat menjauhkan mereka dari situs yang tidak pantas. Admin sebaiknya menonaktifkan mode Samaran agar siswa tidak dapat mengakali filter web.
- **Mode proxy**
  Meskipun sebagian sekolah mungkin menggunakan proxy untuk pemfilteran web, sebaiknya admin mencegah pengguna mengubah sendiri setelan proxy.
- **Akses multi-login**
  Om användarna får logga in på ett sekundärt konto samtidigt som de använder skolans Chromebooks och Workspace-konton kan användaren enkelt stjäla känsliga elev- eller skoluppgifter till det sekundära kontot. Administratörerna bör överväga att blockera åtkomst med multiinloggning.
- **Histori browser**
  Untuk siswa, mungkin akan lebih baik jika admin menonaktifkan kemampuan mereka untuk menghapus histori penjelajahan. Jika terjadi insiden keamanan internet, log histori tersebut akan berguna selama penyelidikan.

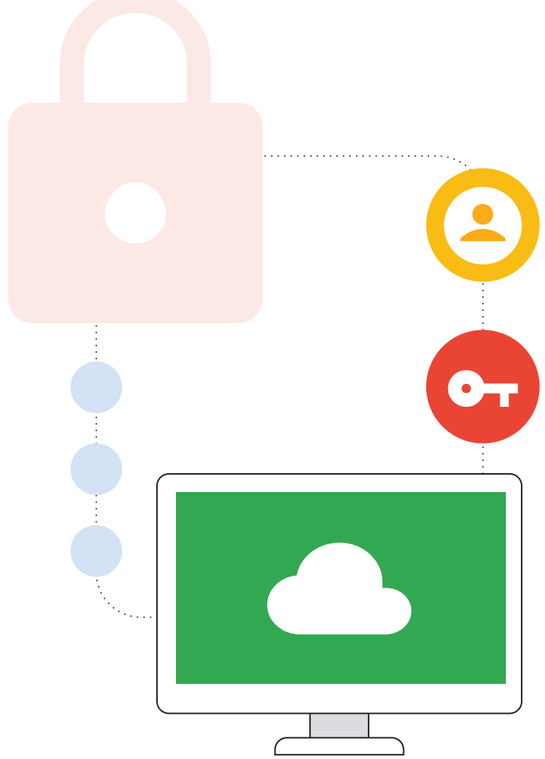
Daftar di atas merupakan titik awal yang bagus untuk memastikan keamanan jaringan sekolah Anda dari jenis-jenis kesalahan paling umum yang dapat menimbulkan insiden siber yang signifikan. Rekomendasi kebijakan keamanan lainnya dapat ditemukan di Checklist Keamanan kami.

Pengelolaan endpoint untuk penggunaan yang aman kapan saja, di mana saja

Sistem pengelolaan kebijakan jarak jauh ChromeOS memungkinkan administrator sekolah menerapkan setelan keamanan dan menjalankan alat keamanan seperti sistem pemfilteran konten di perangkat, bukan di server jaringan sekolah. Dengan begitu, siswa dapat menikmati manfaat keamanan yang sama saat menggunakan Chromebook sekolah, baik di rumah maupun di kelas. Hal ini makin penting saat sekolah bermigrasi ke arah buku pelajaran digital dan alat pembelajaran online, serta perlu mengizinkan siswa membawa pulang komputer untuk mengerjakan pekerjaan rumah mereka..

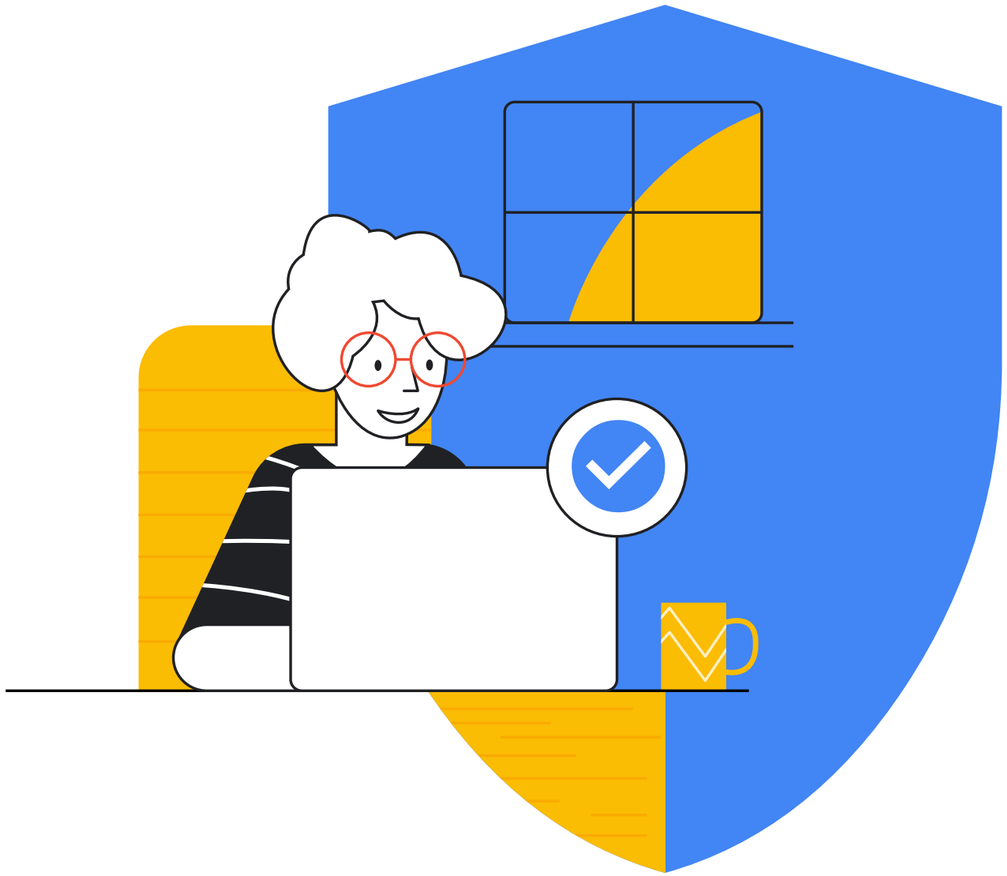
Kesimpulan

Mengamankan institusi sekolah dasar dan menengah dari insiden siber merupakan upaya yang kompleks, tetapi investasi tersebut akan memberikan hasil yang sepadan dalam melindungi diri Anda, siswa, pengajar, staf, dan ekosistem online yang lebih luas. Hal-hal yang dibahas dalam dokumen ini dapat menjadi titik awal yang bagus, tetapi setiap sekolah perlu menyesuaikan rekomendasi yang diberikan di sini dengan kebutuhan unik mereka, serta terus mengimbangi kemunculan berbagai jenis ancaman baru dan teknologi baru. Dokumen ini merupakan fondasi yang solid bagi program keamanan sekolah dasar dan menengah, dilengkapi dengan referensi untuk langkah potensial berikutnya dan item tindakan yang dapat diimplementasikan. Google juga memiliki aneka referensi, pelatihan, serta profesional pengamanan siber terampil yang dapat membantu sekolah dan organisasi menerapkan panduan ini dan memanfaatkan teknologi baru seperti AI. Produk-produk Google yang disesuaikan untuk pendidikan memberikan solusi siap pakai atas beragam masalah pengamanan siber yang dibahas dalam dokumen ini. Kami siap membantu Anda mendesain dan menerapkan program keamanan Anda..



Daftar Referensi

- [1]Google. “Tips untuk Membantu Menjaga Keamanan saat Online.” Pusat Keamanan Google, https://safety.google/intl/id_id/security/security-tips/. Diakses 6 Oktober 2022.
- [2]NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.” NIST Technical Series Publications, 16 April 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Diakses 6 Oktober 2022.
- [3]Microsoft. “Microsoft AccountGuard Program.” Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. Diakses 6 Oktober 2022.
- [4]Google. “Program Perlindungan Lanjutan.” Program Perlindungan Lanjutan Google, https://landing.google.com/intl/id/advancedprotection/. Diakses 6 Oktober 2022.
- [5]Google. “Pusat Keamanan Google.” Pusat Keamanan Google - Stay Safer Online, https://safety.google/intl/id_id/. Diakses 6 Oktober 2022.
- [6]Meta. “Basics: Help Secure Your Account.” Help Secure Your Account, https://www.facebook.com/gpa/resources/basics/security. Diakses 6 Oktober 2022.
- [7]Meta. “Facebook Protect.” Facebook, https://www.facebook.com/gpa/facebook-protect. Diakses 6 Oktober 2022.
- [8]NIST. “SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise.” NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Diakses 6 Oktober 2022.
- Kunci sandi: https://developers.google.com/identity/passkeys?hl=id
- CISA Protecting Our Future Cybersecurity K-12 Report https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO Report https://www.gao.gov/products/gao-20-644
- Untuk informasi selengkapnya tentang cara Google for Education membantu Anda melindungi institusi, lihat Pusat Keamanan dan Privasi Google for Education.
- Zcaler Phishing Report



Google for Education

Safer with Google